FIG.1

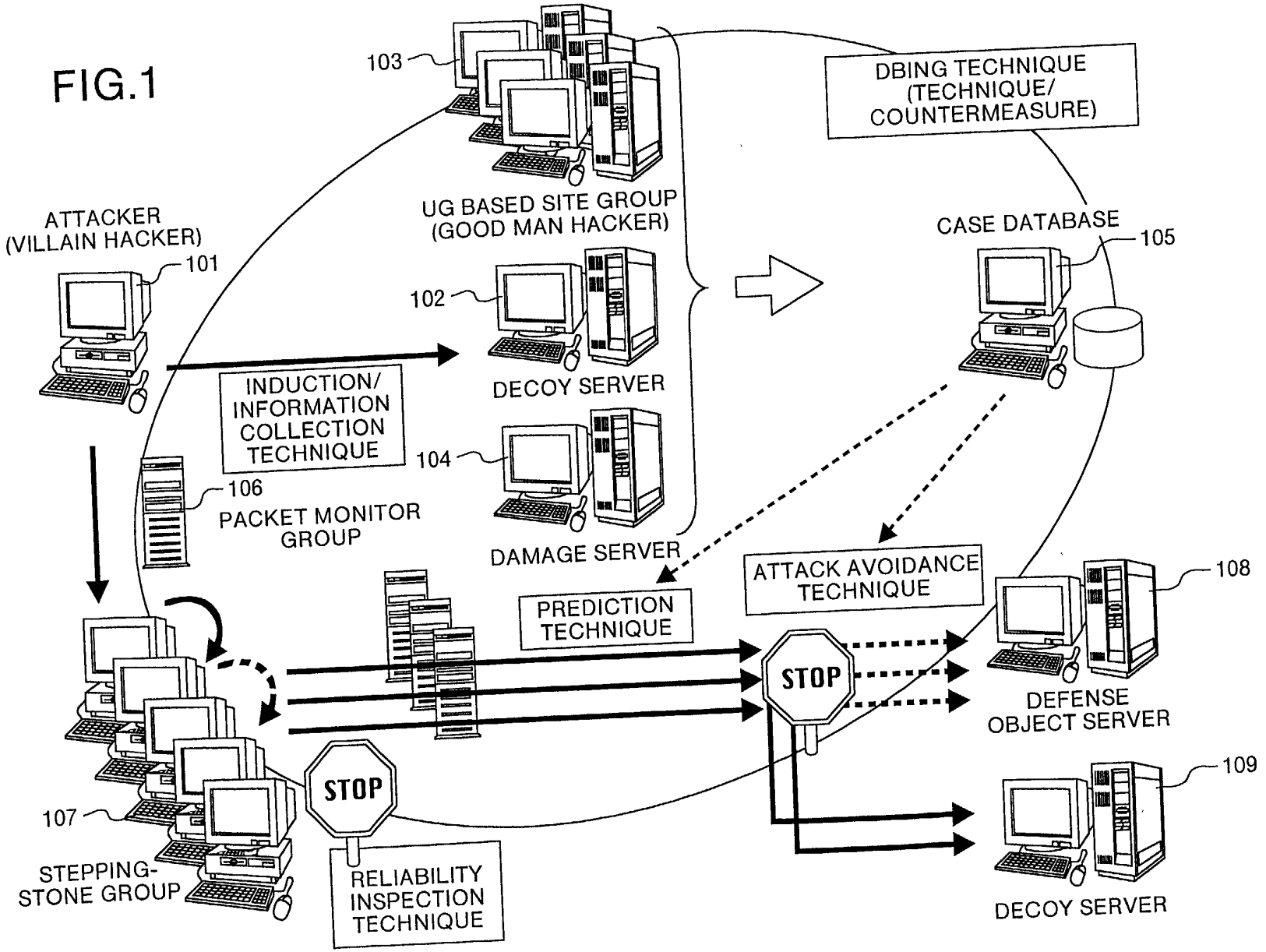

103
UG BASED SITE GROUP
(GOOD MAN HACKER)
DBING TECHNIQUE
(TECHNIQUE/
COUNTERMEASURE)
ATTACKER
(VILLAIN HACKER)
101
102
DECOY SERVER
CASE DATABASE
105
INDUCTION/
INFORMATION
COLLECTION
TECHNIQUE
104
106
PACKET MONITOR
GROUP
DAMAGE SERVER
PREDICTION
TECHNIQUE
ATTACK AVOIDANCE
TECHNIQUE
108
STOP
DEFENSE
OBJECT SERVER
STOP
107
STEPPING-
STONE GROUP
RELIABILITY
INSPECTION
TECHNIQUE
109
DECOY SERVER

FIG.2

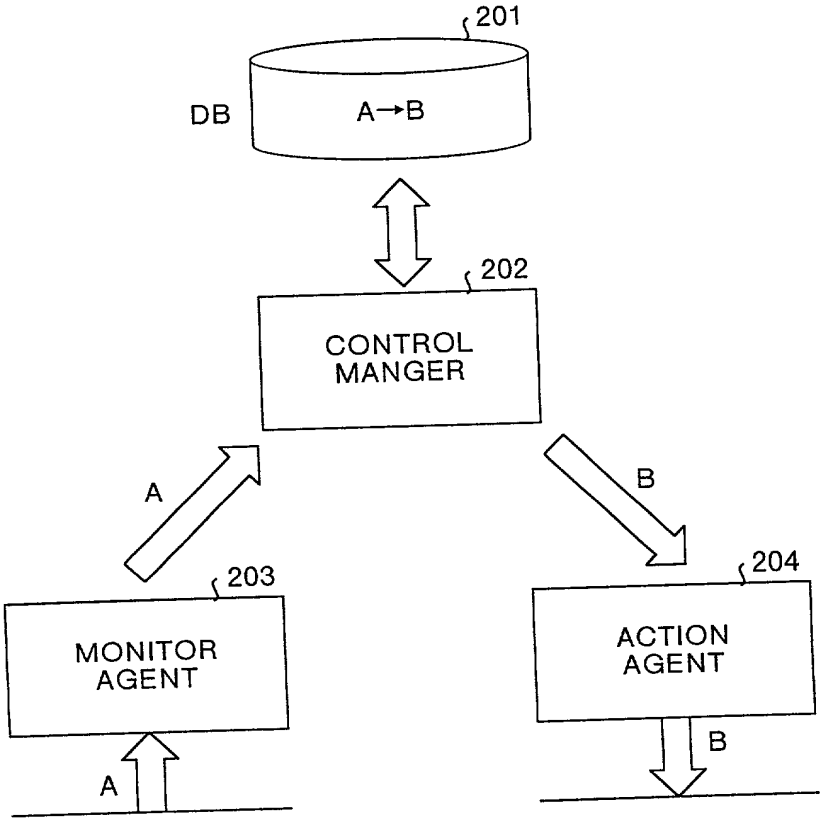

201
DB
A→B
202
CONTROL MANGER
A
B
203
MONITOR AGENT
204
ACTION AGENT
A
B

FIG.3

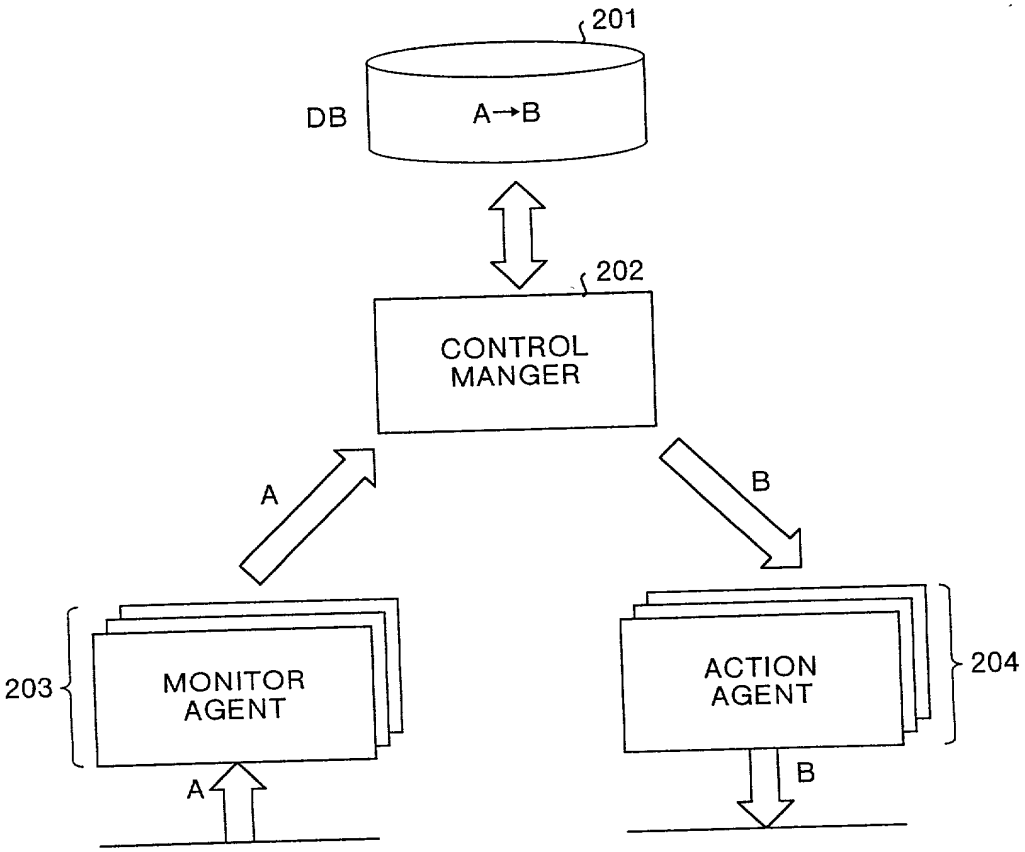

201
DB
A→B
202
CONTROL MANGER
A
B
203
MONITOR AGENT
A
ACTION AGENT
204
B

FIG.4

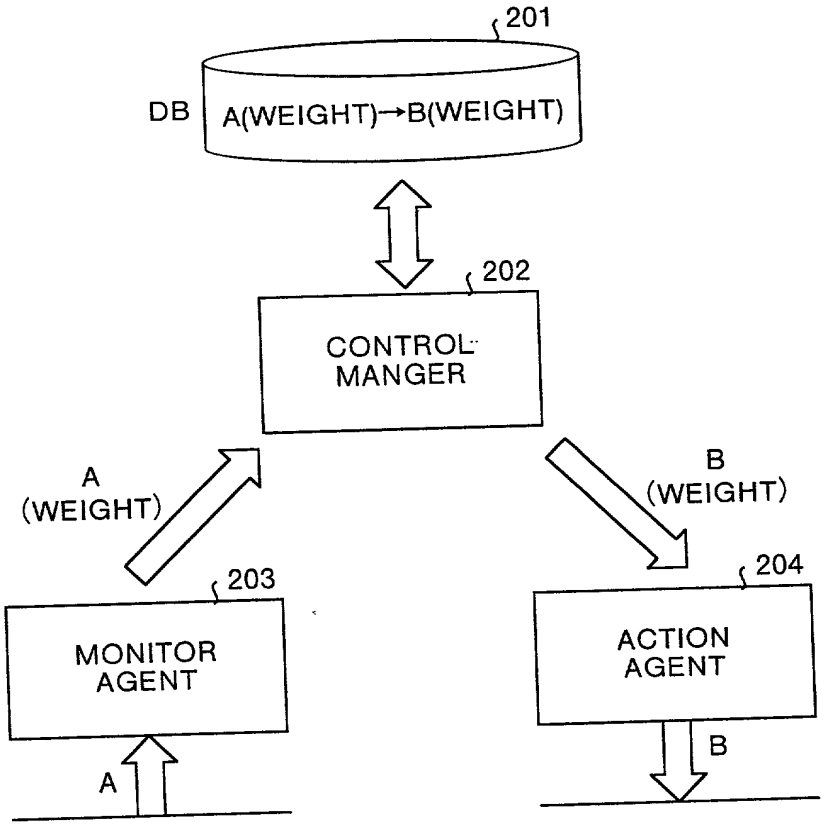
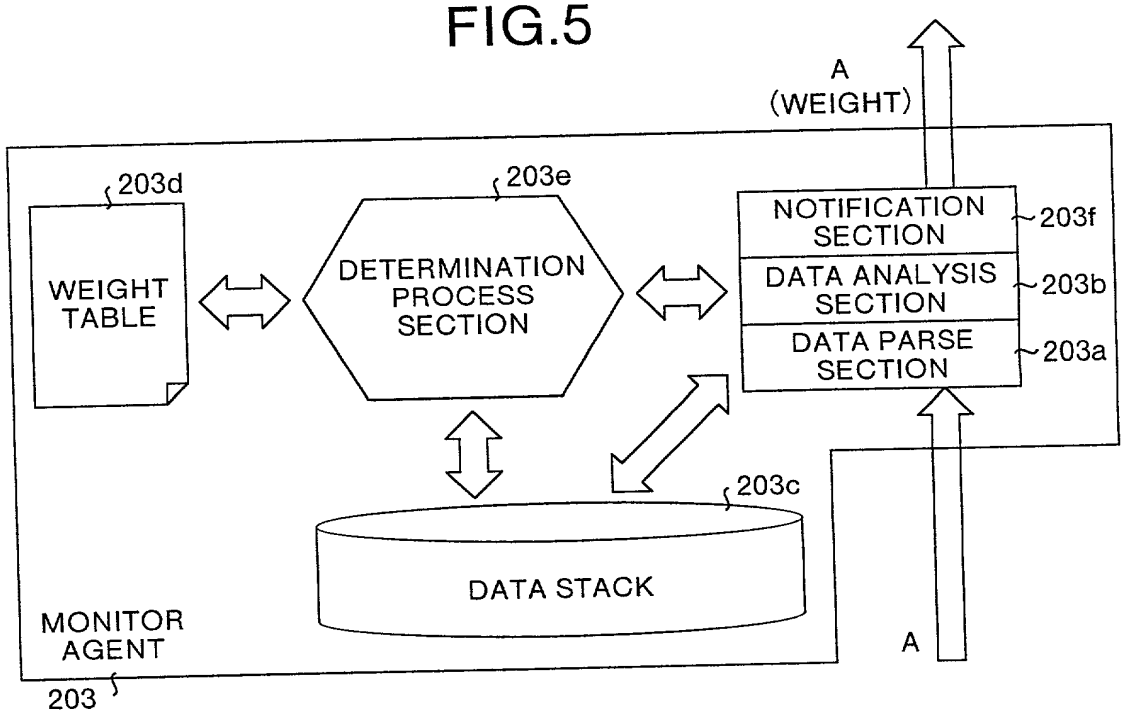

201
DB
A(WEIGHT)→B(WEIGHT)
202
CONTROL MANGER
A
(WEIGHT)
B
(WEIGHT)
203
MONITOR AGENT
204
ACTION AGENT
A
B

FIG.5



JP2006-268568A

FIG.6

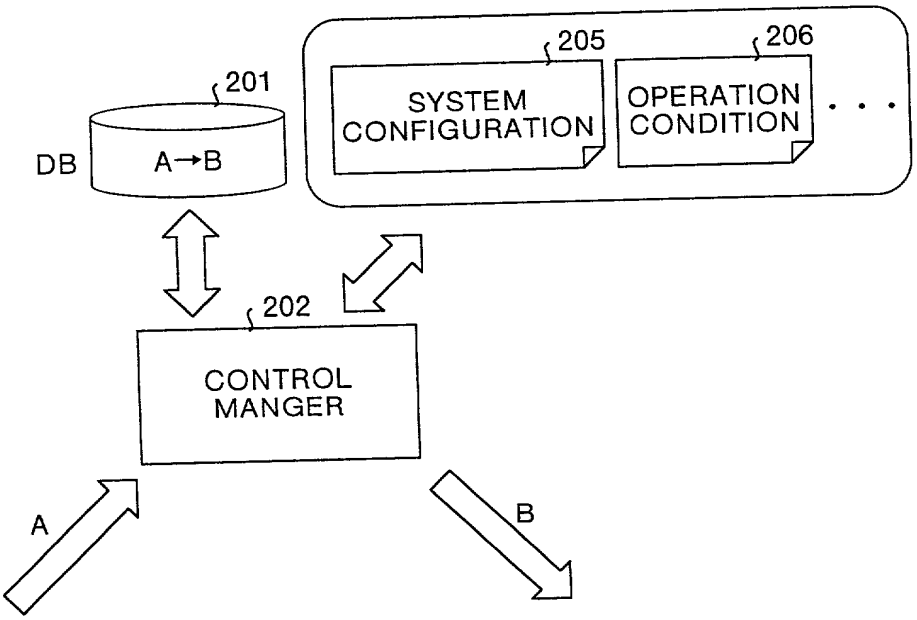
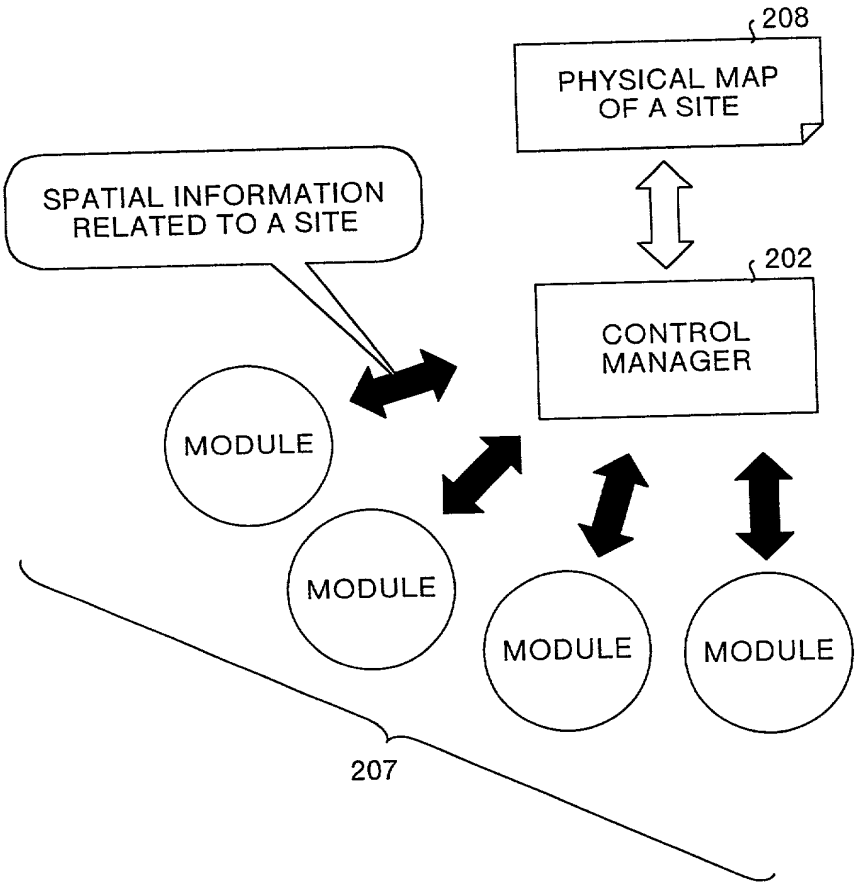

201
205
206
SYSTEM CONFIGURATION
OPERATION CONDITION
DB
A→B
202
CONTROL MANGER
A
B

FIG.7



0969678-080802

FIG.8

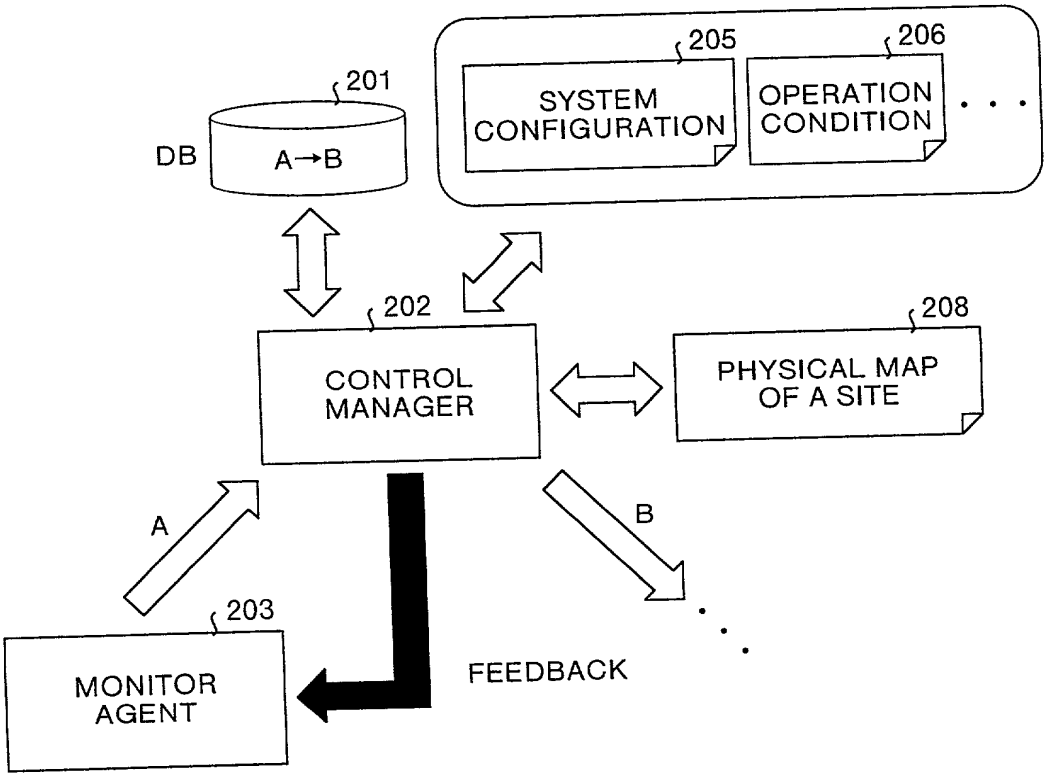

201
DB
A→B
205
SYSTEM CONFIGURATION
206
OPERATION CONDITION
202
CONTROL MANAGER
208
PHYSICAL MAP OF A SITE
A
B
203
MONITOR AGENT
FEEDBACK

FIG.9

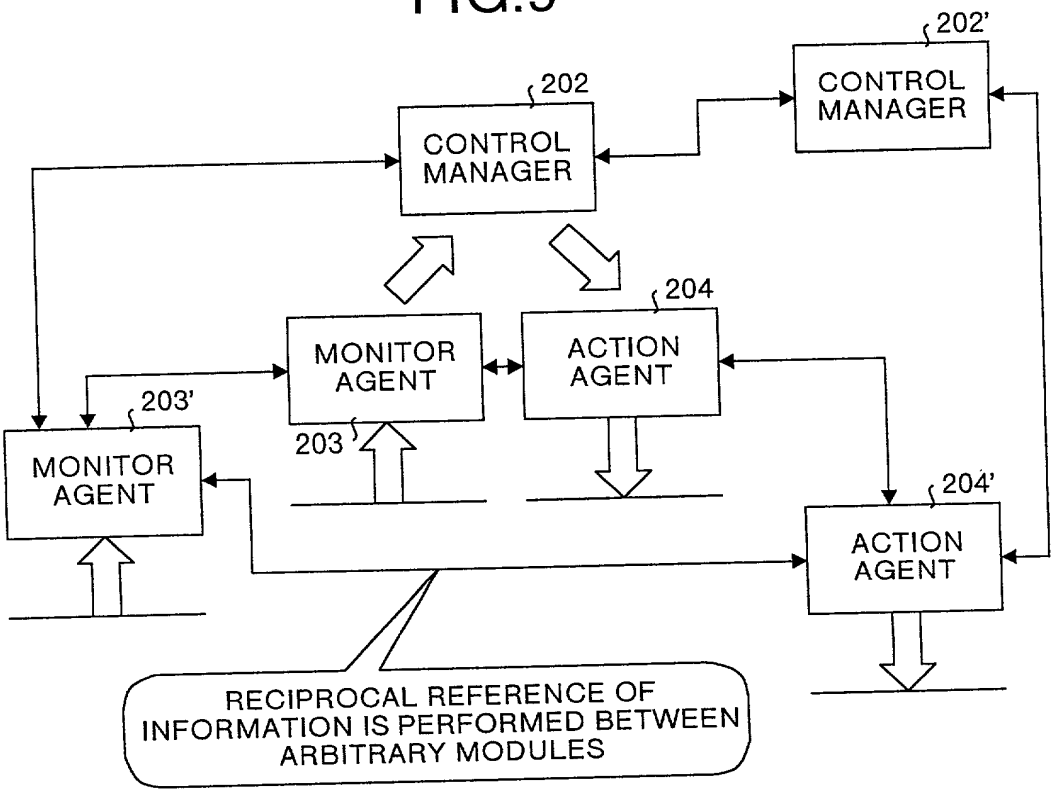

202'
CONTROL MANAGER
202
CONTROL MANAGER
204
MONITOR AGENT
ACTION AGENT
203'
203
MONITOR AGENT
204'
ACTION AGENT
RECIPROCAL REFERENCE OF INFORMATION IS PERFORMED BETWEEN ARBITRARY MODULES

FIG.10

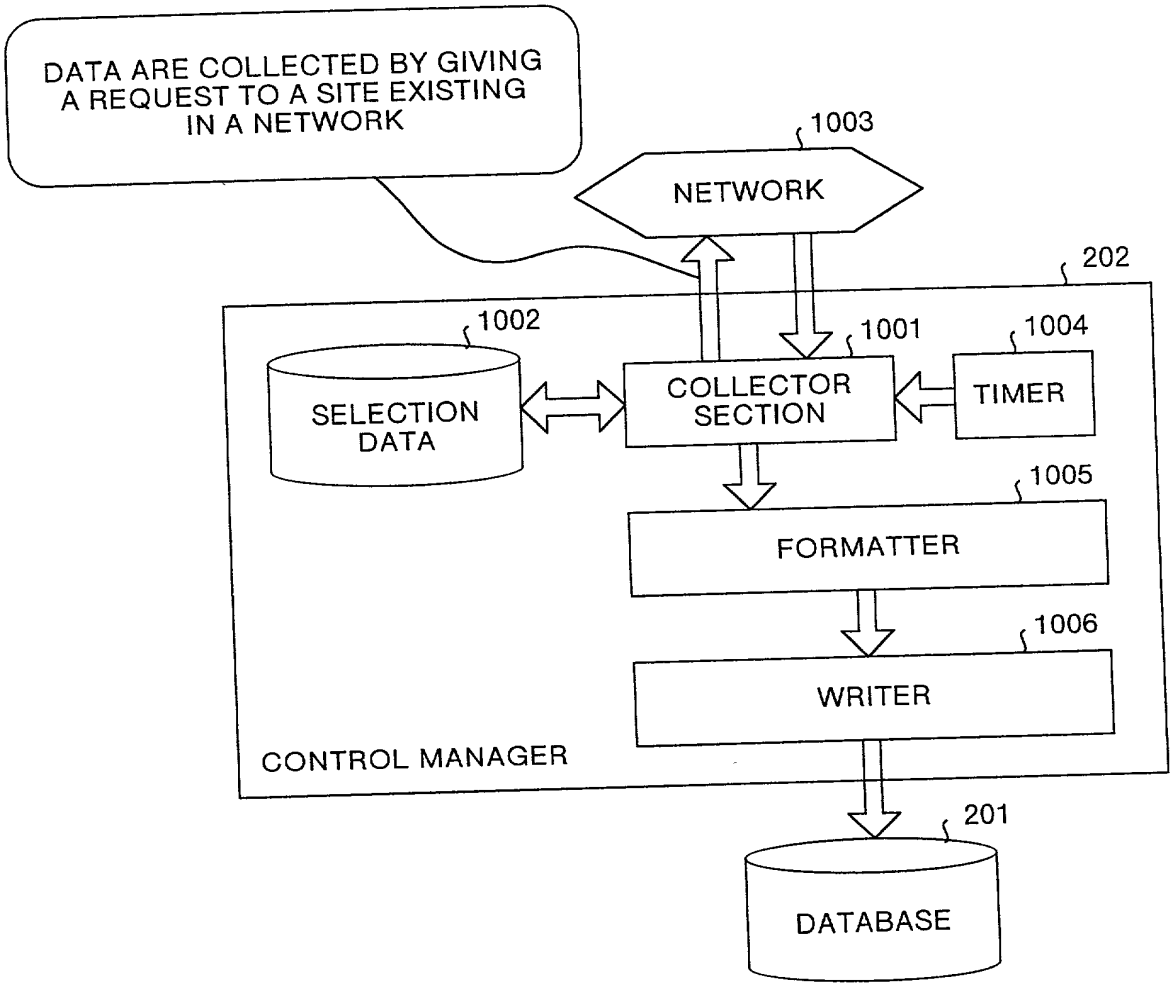
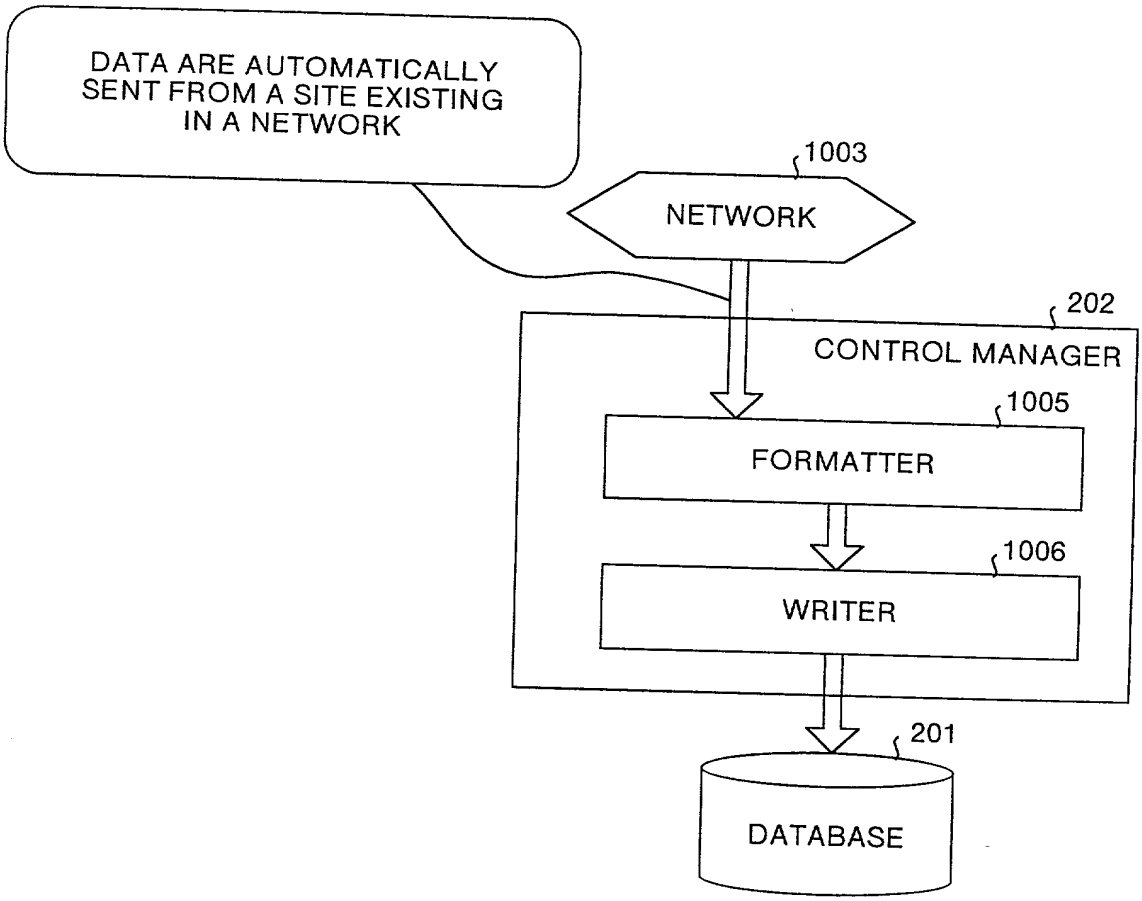
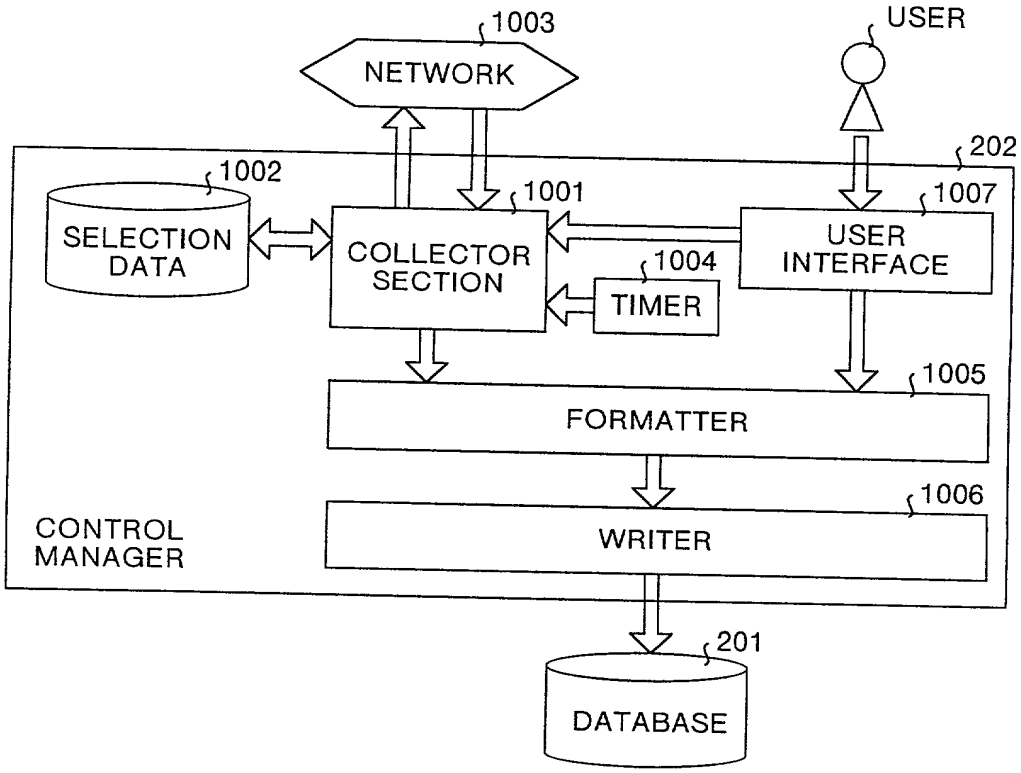

DATA ARE COLLECTED BY GIVING A REQUEST TO A SITE EXISTING IN A NETWORK
1003
NETWORK
202
1002
SELECTION DATA
1001
COLLECTOR SECTION
1004
TIMER
1005
FORMATTER
1006
WRITER
CONTROL MANAGER
201
DATABASE

FIG.11



EP 1 209 595 A2

FIG.12



EP 0 956 528 B1

FIG.13

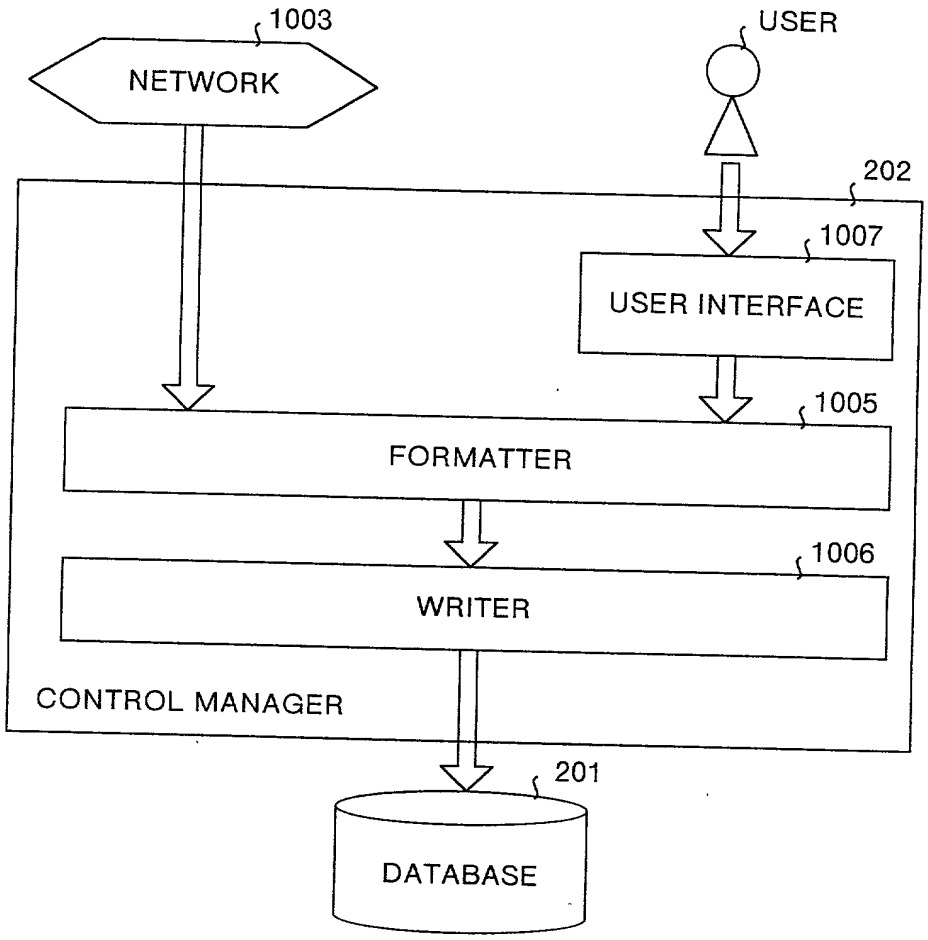

1003
NETWORK
USER
202
1007
USER INTERFACE
1005
FORMATTER
1006
WRITER
CONTROL MANAGER
201
DATABASE

FIG.14

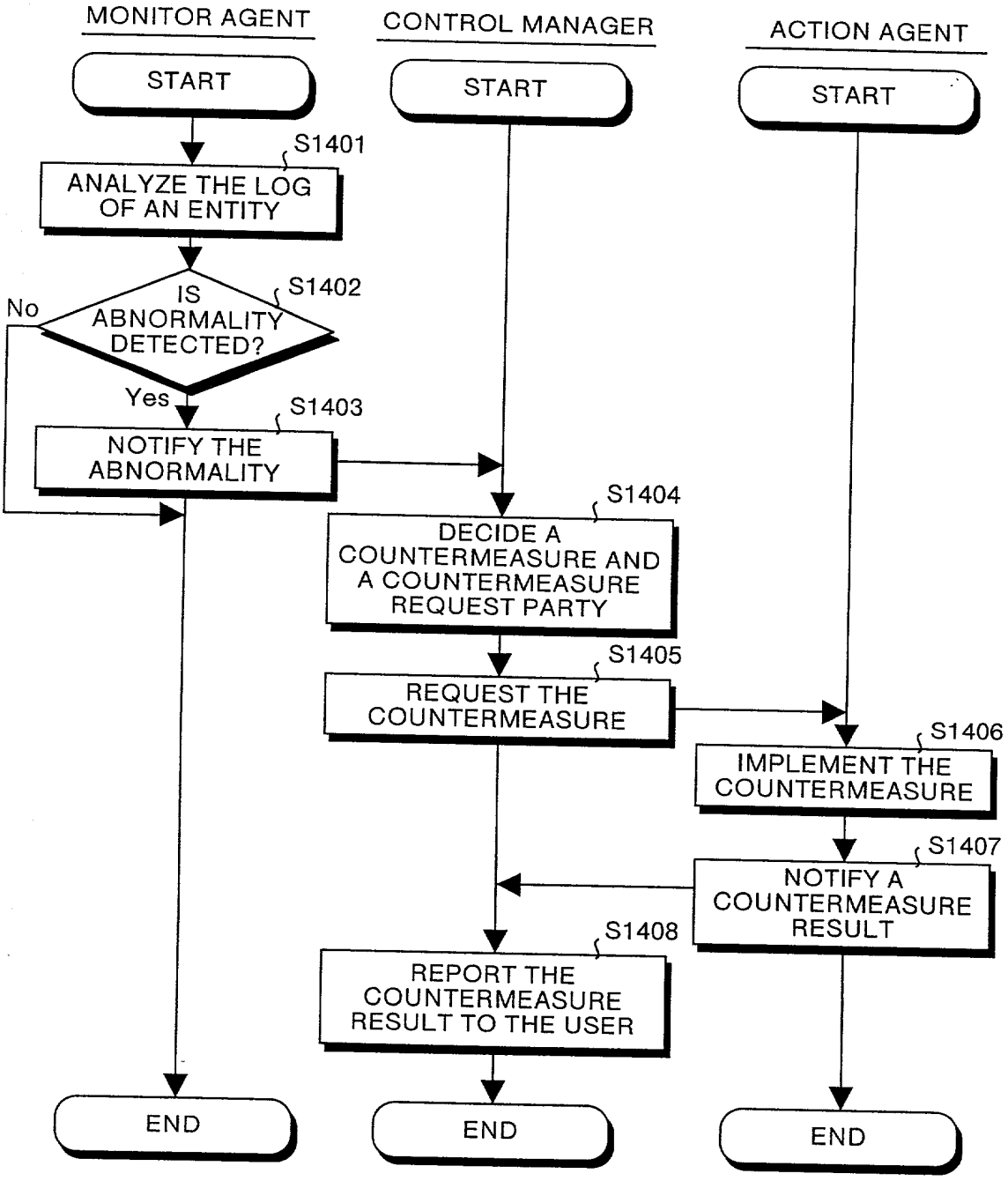

MONITOR AGENT
CONTROL MANAGER
ACTION AGENT
START
START
START
S1401
ANALYZE THE LOG OF AN ENTITY
S1402
IS ABNORMALITY DETECTED?
No
Yes
S1403
NOTIFY THE ABNORMALITY
S1404
DECIDE A COUNTERMEASURE AND A COUNTERMEASURE REQUEST PARTY
S1405
REQUEST THE COUNTERMEASURE
S1406
IMPLEMENT THE COUNTERMEASURE
S1407
NOTIFY A COUNTERMEASURE RESULT
S1408
REPORT THE COUNTERMEASURE RESULT TO THE USER
END
END
END

FIG.15

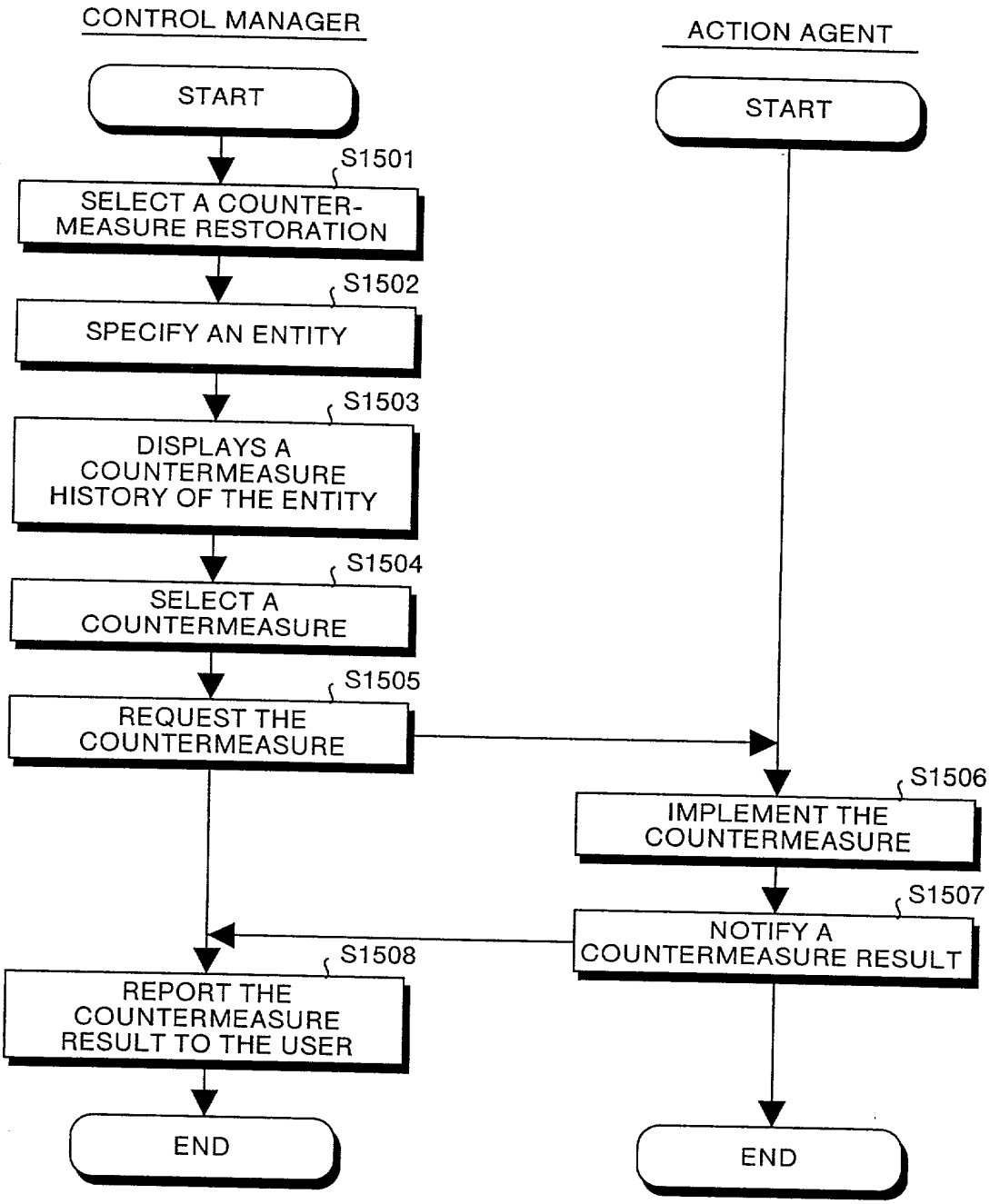

CONTROL MANAGER
ACTION AGENT
START
START
S1501
SELECT A COUNTER-MEASURE RESTORATION
S1502
SPECIFY AN ENTITY
S1503
DISPLAYS A COUNTERMEASURE HISTORY OF THE ENTITY
S1504
SELECT A COUNTERMEASURE
S1505
REQUEST THE COUNTERMEASURE
S1506
IMPLEMENT THE COUNTERMEASURE
S1507
NOTIFY A COUNTERMEASURE RESULT
S1508
REPORT THE COUNTERMEASURE RESULT TO THE USER
END
END

FIG.16

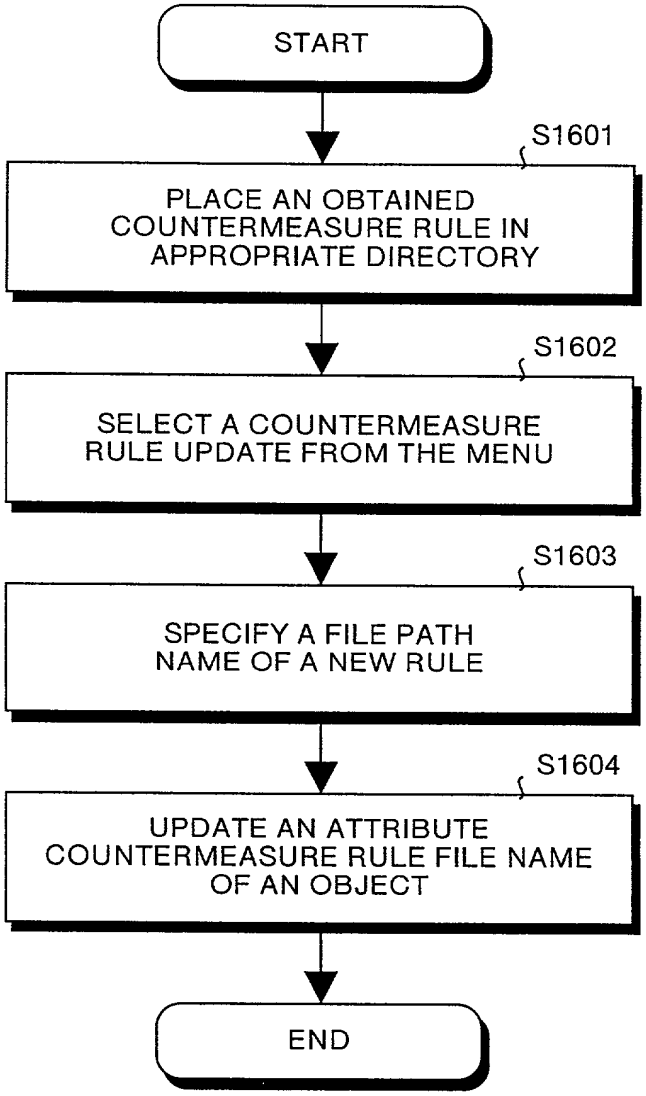
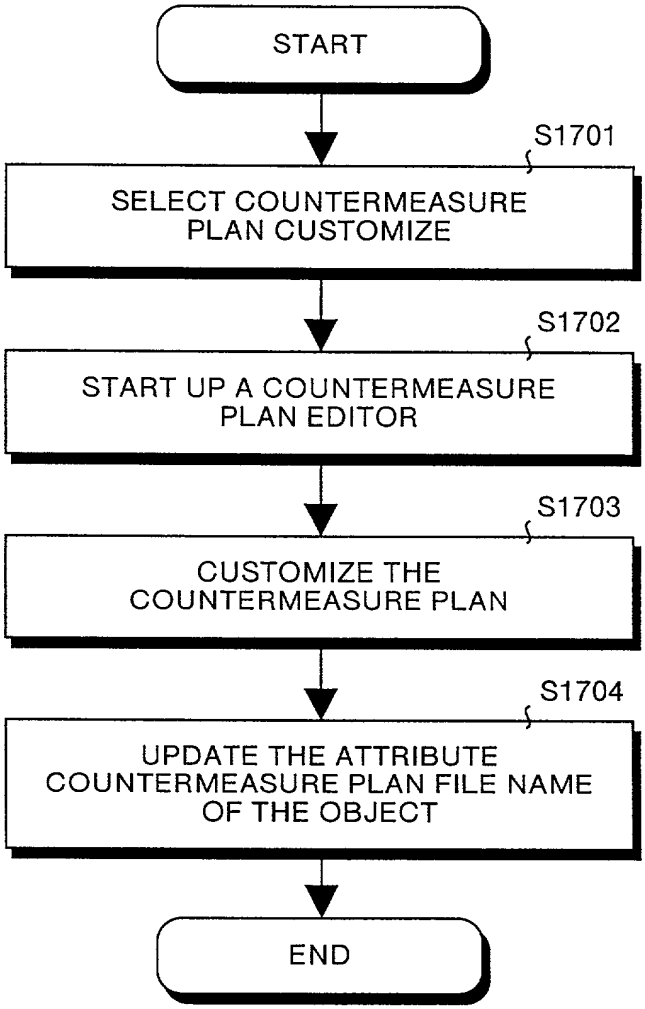
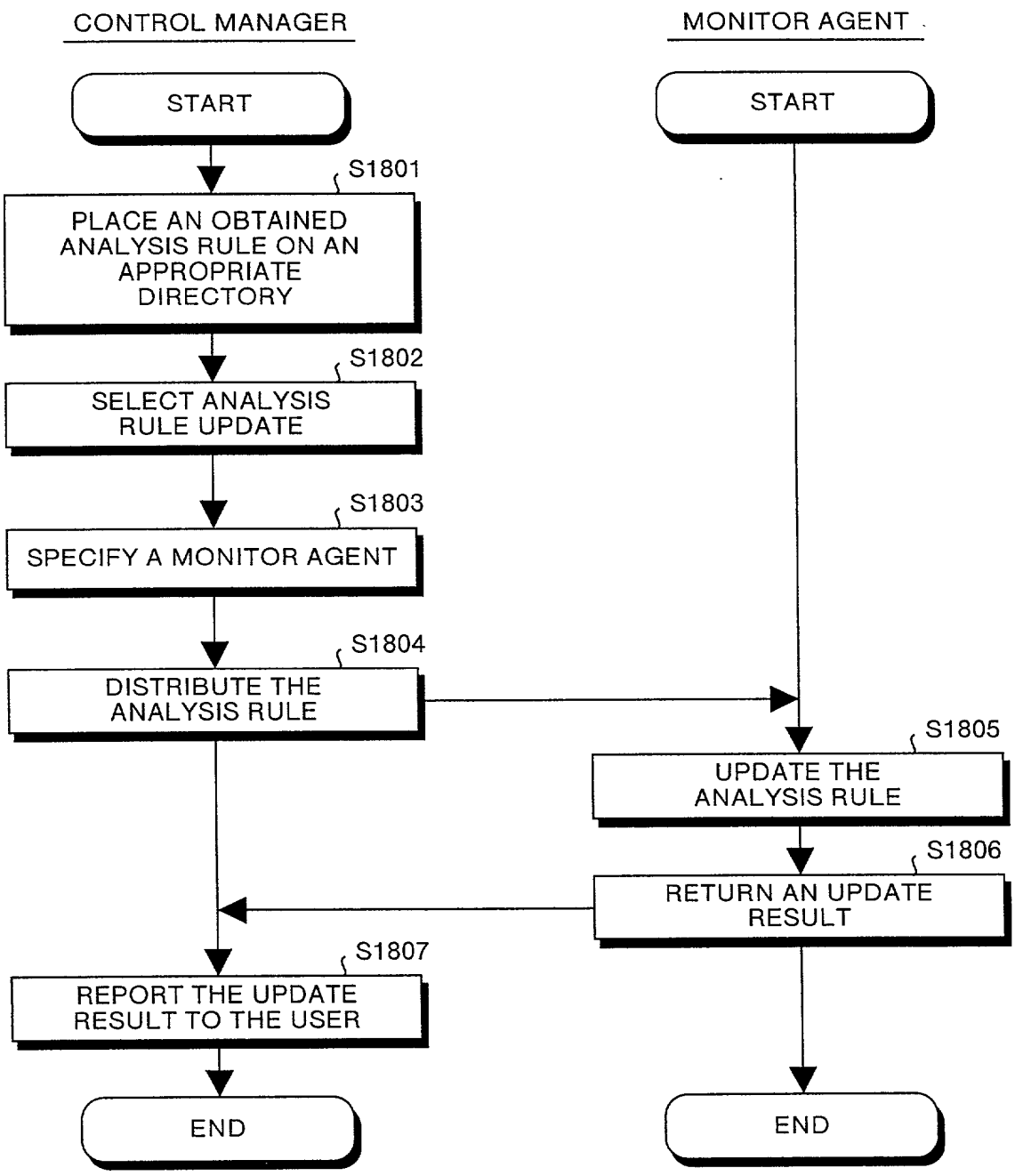

START
S1601
PLACE AN OBTAINED COUNTERMEASURE RULE IN APPROPRIATE DIRECTORY
S1602
SELECT A COUNTERMEASURE RULE UPDATE FROM THE MENU
S1603
SPECIFY A FILE PATH NAME OF A NEW RULE
S1604
UPDATE AN ATTRIBUTE COUNTERMEASURE RULE FILE NAME OF AN OBJECT
END

FIG.17



EP 2 696 299 A1

FIG.18



EP 2 056 212 A1

FIG.19

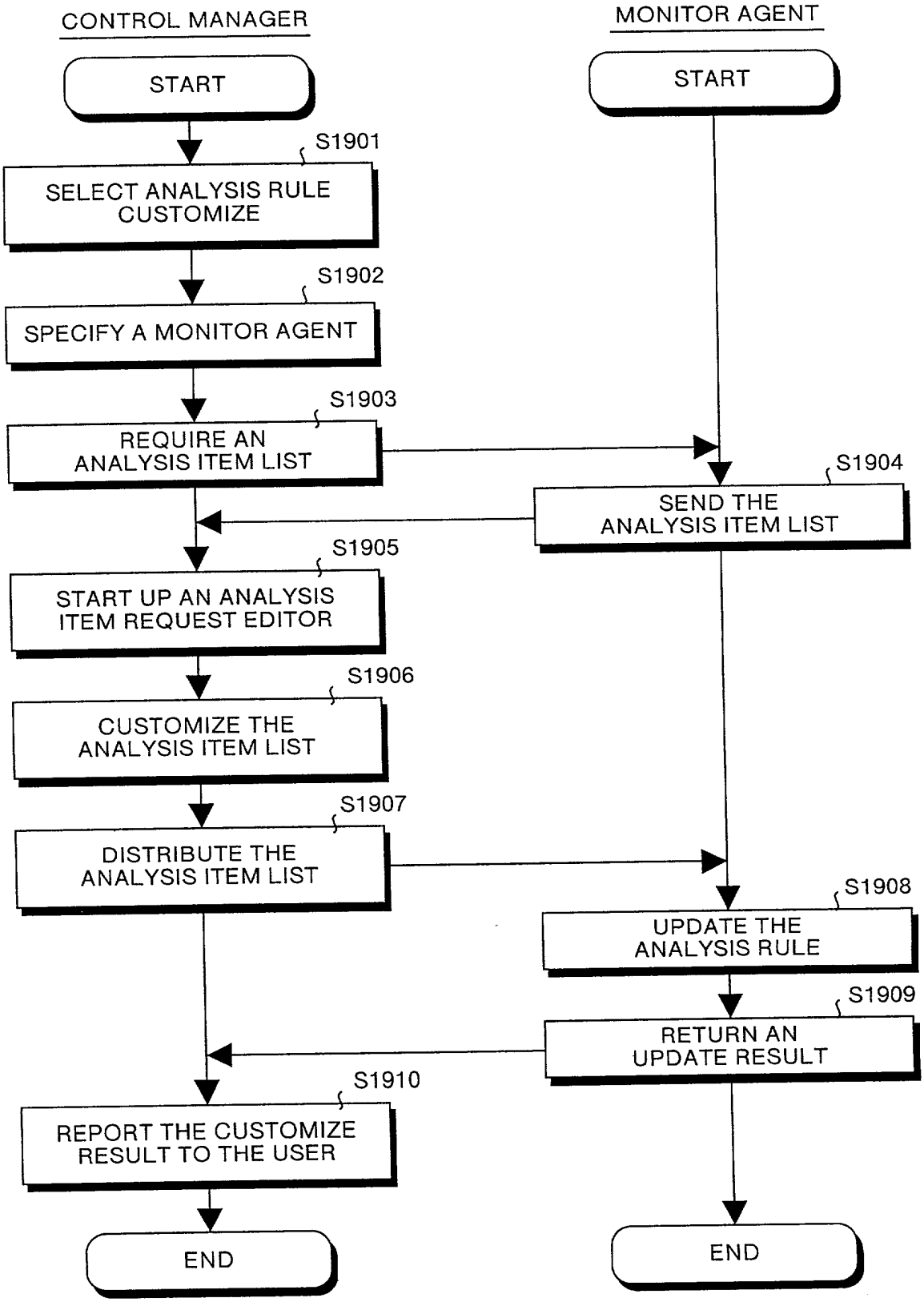
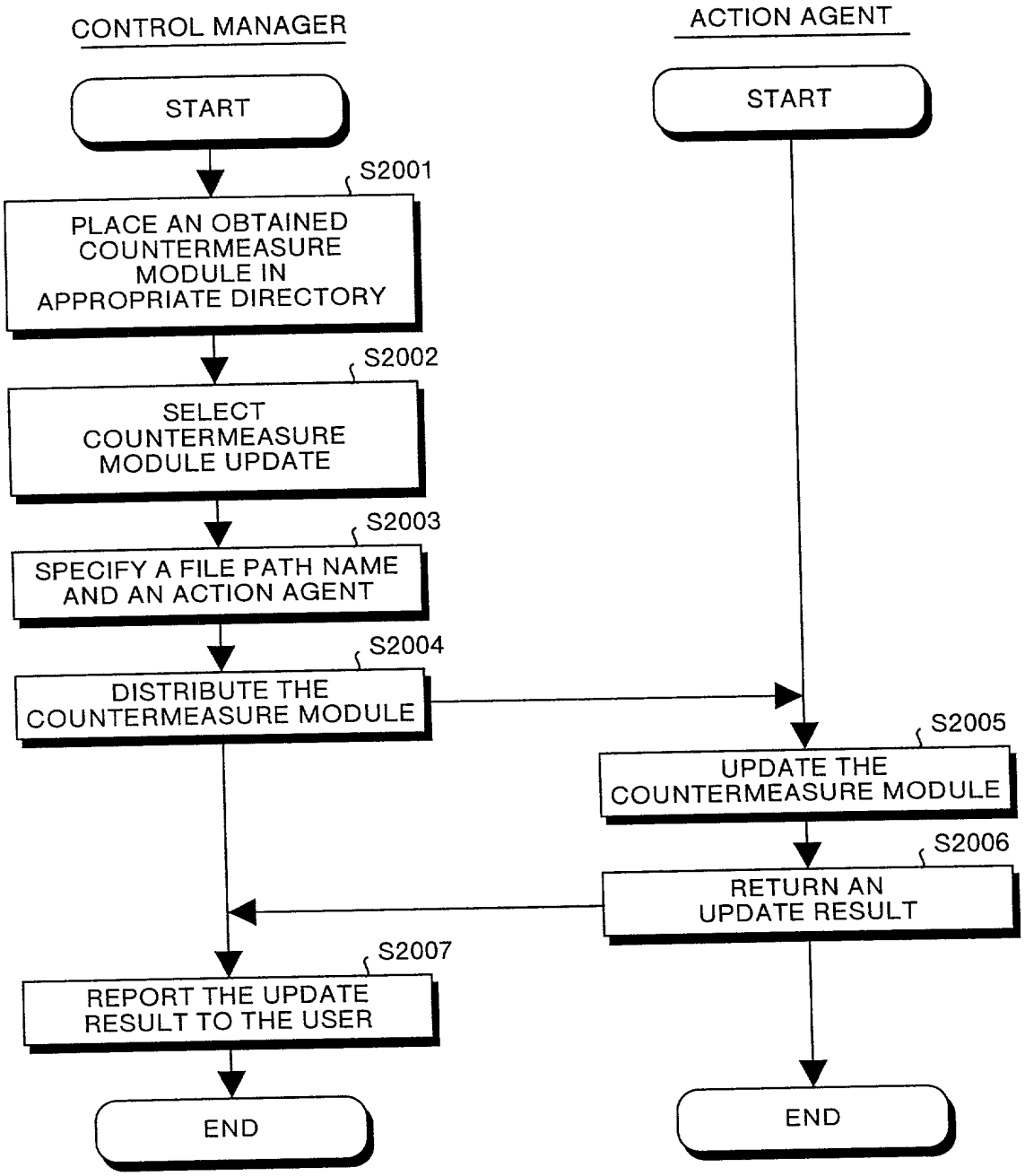

CONTROL MANAGER
MONITOR AGENT
START
START
S1901
SELECT ANALYSIS RULE CUSTOMIZE
S1902
SPECIFY A MONITOR AGENT
S1903
REQUIRE AN ANALYSIS ITEM LIST
S1904
SEND THE ANALYSIS ITEM LIST
S1905
START UP AN ANALYSIS ITEM REQUEST EDITOR
S1906
CUSTOMIZE THE ANALYSIS ITEM LIST
S1907
DISTRIBUTE THE ANALYSIS ITEM LIST
S1908
UPDATE THE ANALYSIS RULE
S1909
RETURN AN UPDATE RESULT
S1910
REPORT THE CUSTOMIZE RESULT TO THE USER
END
END

FIG.20



Page 2 of 56 - 2/6/2006 5:56:39 PM

FIG.21A

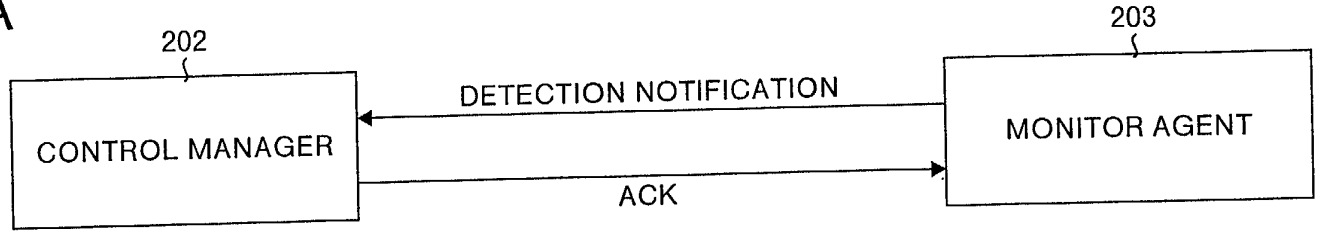


FIG.21B

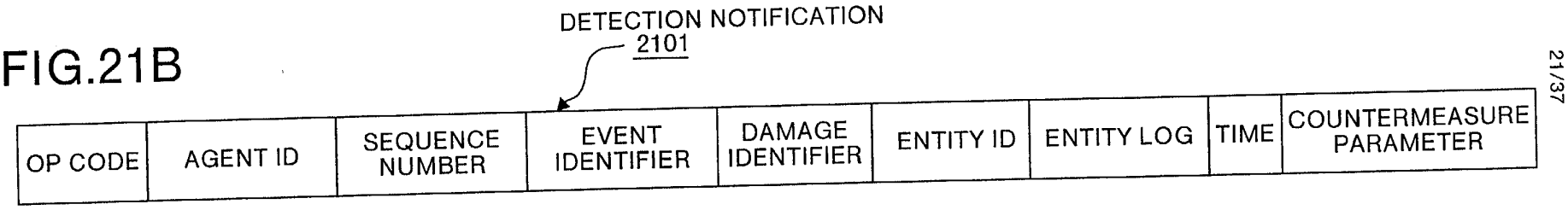


FIG.21C

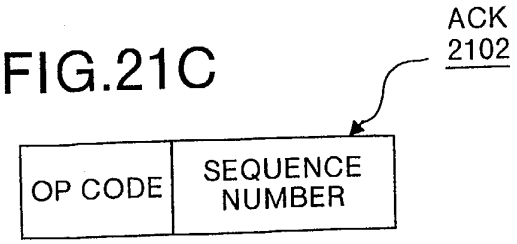


FIG.22A

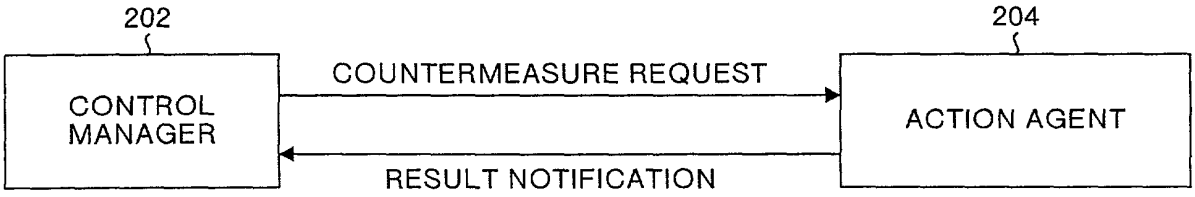


FIG.22B

COUNTERMEASURE REQUEST
2201

OP CODE	AGENT ID	SEQUENCE NUMBER	ENTITY ID	COUNTER-MEASURE IDENTIFIER	COUNTER-MEASURE PARAMETER

FIG.22C

RESULT NOTIFICATION
2202

OP CODE	SEQUENCE NUMBER	ENTITY ID	RETURN VALUE	ERROR CODE

FIG.23A

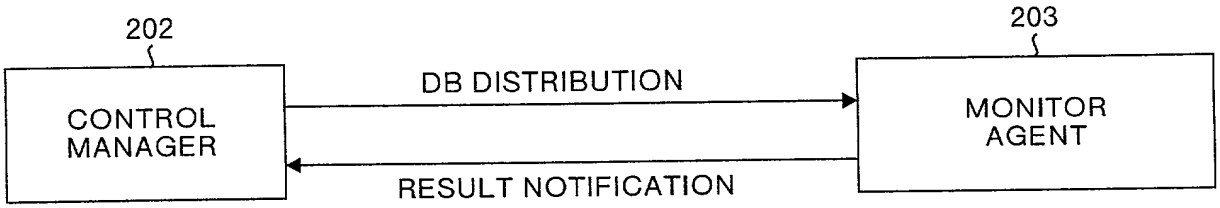


FIG.23B

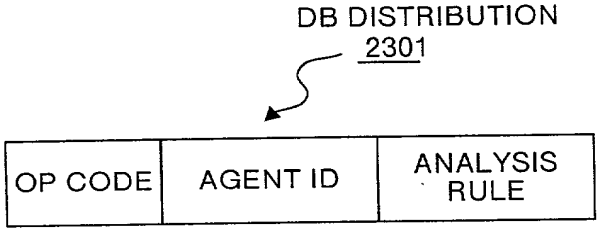


FIG.23C

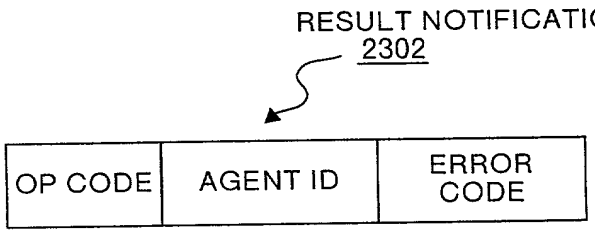


FIG.24A

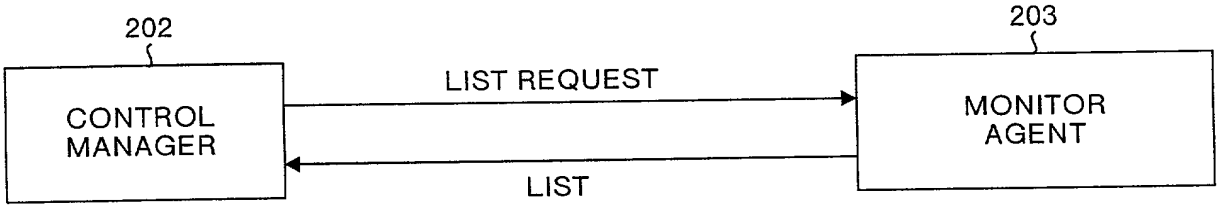


FIG.24B

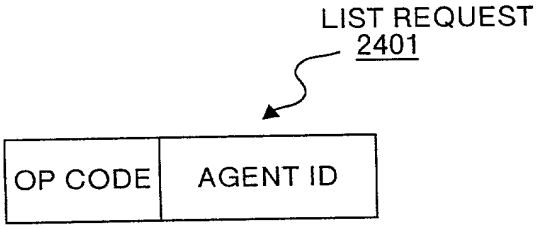


FIG.24C

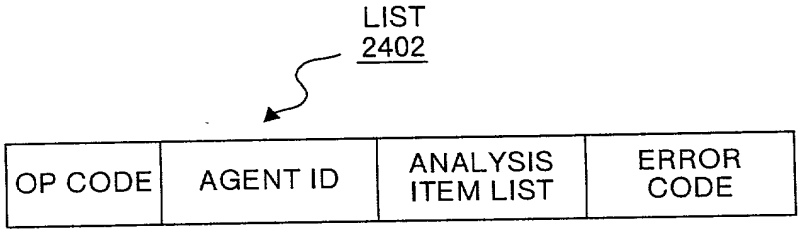


FIG.25A

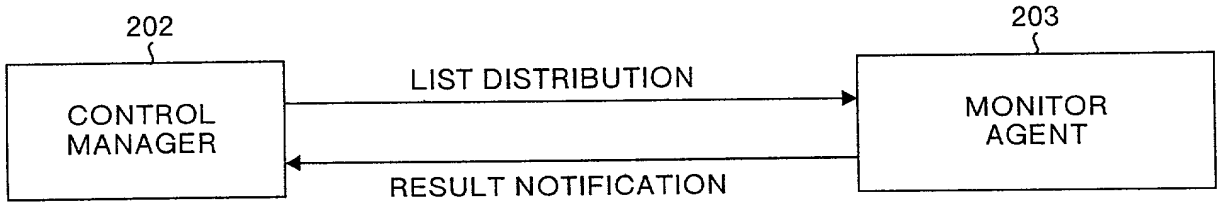


FIG.25B

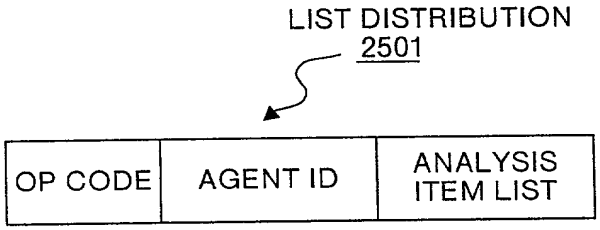
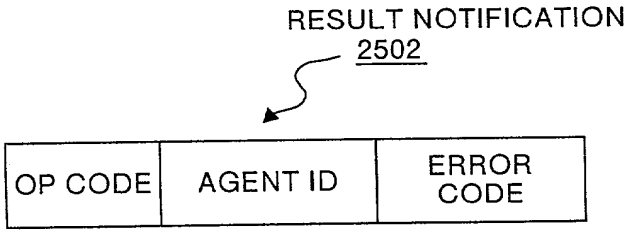


FIG.25C



JP2003-256269

FIG.26A

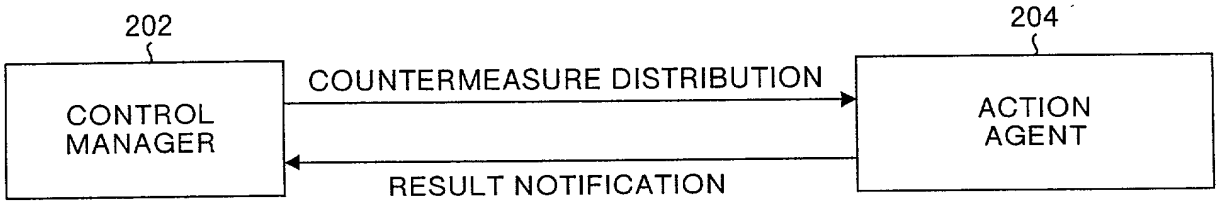


FIG.26B

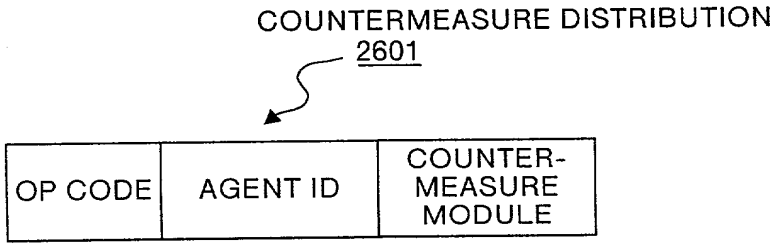


FIG.26C

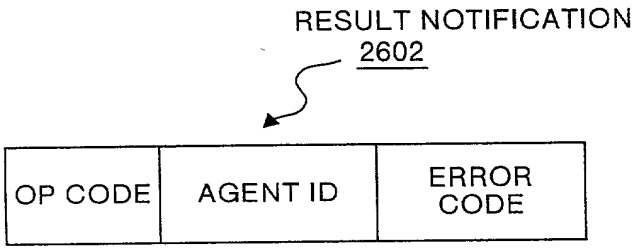


FIG.27

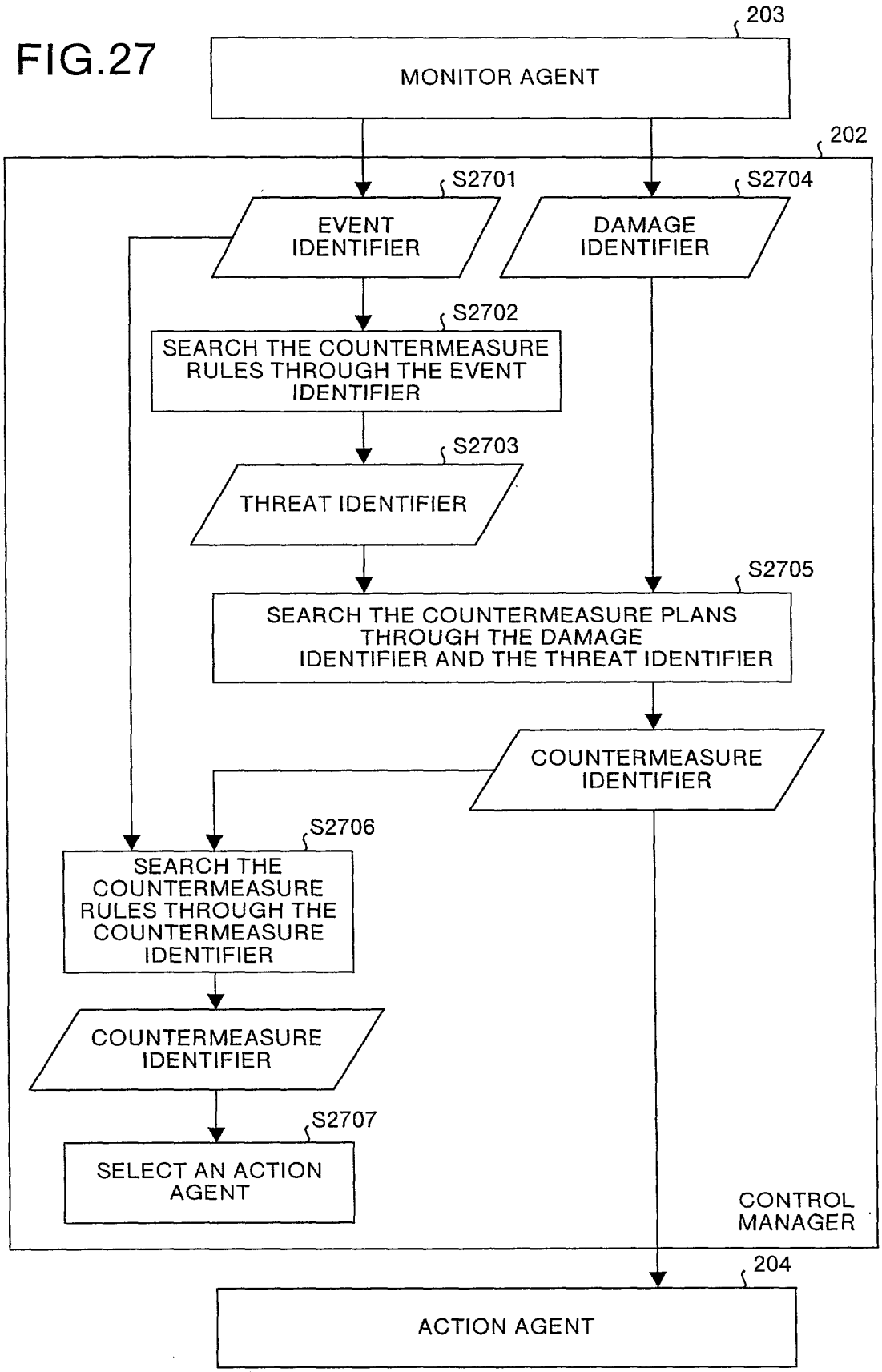

203
MONITOR AGENT
202
S2701
EVENT IDENTIFIER
S2704
DAMAGE IDENTIFIER
S2702
SEARCH THE COUNTERMEASURE RULES THROUGH THE EVENT IDENTIFIER
S2703
THREAT IDENTIFIER
S2705
SEARCH THE COUNTERMEASURE PLANS THROUGH THE DAMAGE IDENTIFIER AND THE THREAT IDENTIFIER
COUNTERMEASURE IDENTIFIER
S2706
SEARCH THE COUNTERMEASURE RULES THROUGH THE COUNTERMEASURE IDENTIFIER
COUNTERMEASURE IDENTIFIER
S2707
SELECT AN ACTION AGENT
CONTROL MANAGER
204
ACTION AGENT

FIG.28A

EVENT IDENTIFIER	DAMAGE IDENTIFIER
EVENT 001	DAMAGE EXISTS

FIG.28B

COUNTERMEASURE RULES

EVENT IDENTIFIER	THREAT IDENTIFIER	COUNTER-MEASURE IDENTIFIER	COUNTER-MEASURE DESIGNATOR
EVENT 001	THREAT 001	COUNTER-MEASURE 001	SERVER
EVENT 001	THREAT 001	COUNTER-MEASURE 002	FW
EVENT 002	THREAT 001	COUNTER-MEASURE 001	SERVER
EVENT 002	THREAT 001	COUNTER-MEASURE 002	FW
EVENT 003	THREAT 010	COUNTER-MEASURE 011	SERVER
EVENT 003	THREAT 010	COUNTER-MEASURE 012	SERVER
EVENT 003	THREAT 010	COUNTER-MEASURE 012	FW
. . .	. . .	. . .	. . .

FIG.28C

COUNTERMEASURE PLANS

EVENT IDENTIFIER	THREAT IDENTIFIER	COUNTER-MEASURE IDENTIFIER
DAMAGE EXISTS	THREAT 001	COUNTER-MEASURE 001
DAMAGE UNCLEAR	THREAT 001	COUNTER-MEASURE 002
NO DAMAGE	THREAT 001	—
DAMAGE EXISTS	THREAT 002	COUNTER-MEASURE 011
DAMAGE UNCLEAR	THREAT 002	—
NO DAMAGE	THREAT 002	—
. . .	. . .	. . .

FIG.28D

COUNTERMEASURE RULES

EVENT IDENTIFIER	THREAT IDENTIFIER	COUNTER-MEASURE IDENTIFIER	COUNTER-MEASURE DESIGNATOR
EVENT 001	THREAT 001	COUNTER-MEASURE 001	SERVER
EVENT 001	THREAT 001	COUNTER-MEASURE 002	FW
EVENT 002	THREAT 001	COUNTER-MEASURE 001	SERVER
EVENT 002	THREAT 001	COUNTER-MEASURE 002	FW
EVENT 003	THREAT 010	COUNTER-MEASURE 011	SERVER
EVENT 003	THREAT 010	COUNTER-MEASURE 012	SERVER
EVENT 003	THREAT 010	COUNTER-MEASURE 012	FW
. . .	. . .	. . .	. . .

EP 2 955 652 A1 09-12-2015

FIG.29

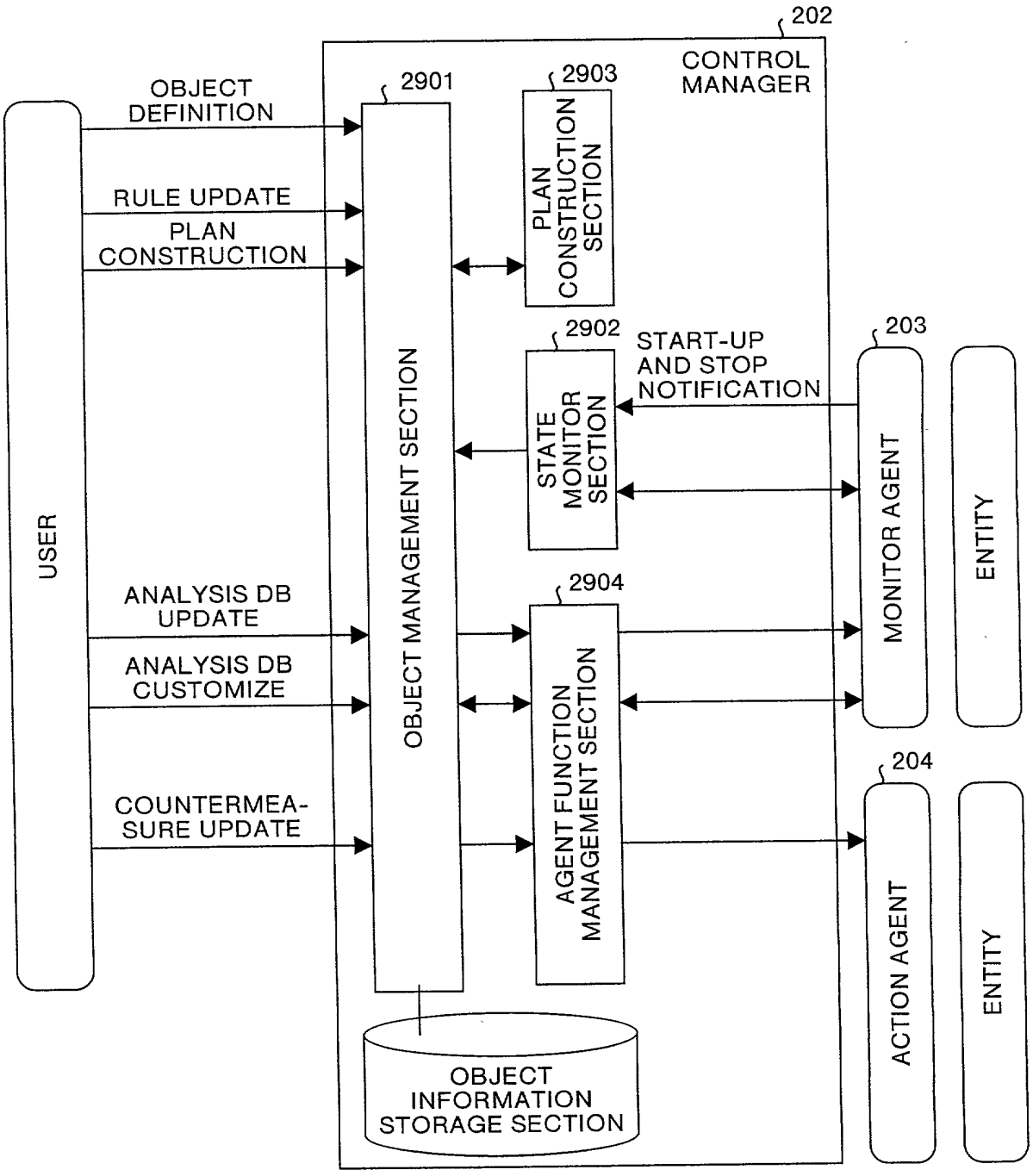

202
CONTROL MANAGER
2901
2903
OBJECT DEFINITION
RULE UPDATE
PLAN CONSTRUCTION
PLAN CONSTRUCTION SECTION
2902
START-UP AND STOP NOTIFICATION
203
STATE MONITOR SECTION
MONITOR AGENT
ENTITY
USER
OBJECT MANAGEMENT SECTION
2904
ANALYSIS DB UPDATE
ANALYSIS DB CUSTOMIZE
AGENT FUNCTION MANAGEMENT SECTION
204
COUNTERMEA-SURE UPDATE
ACTION AGENT
ENTITY
OBJECT INFORMATION STORAGE SECTION

FIG.30

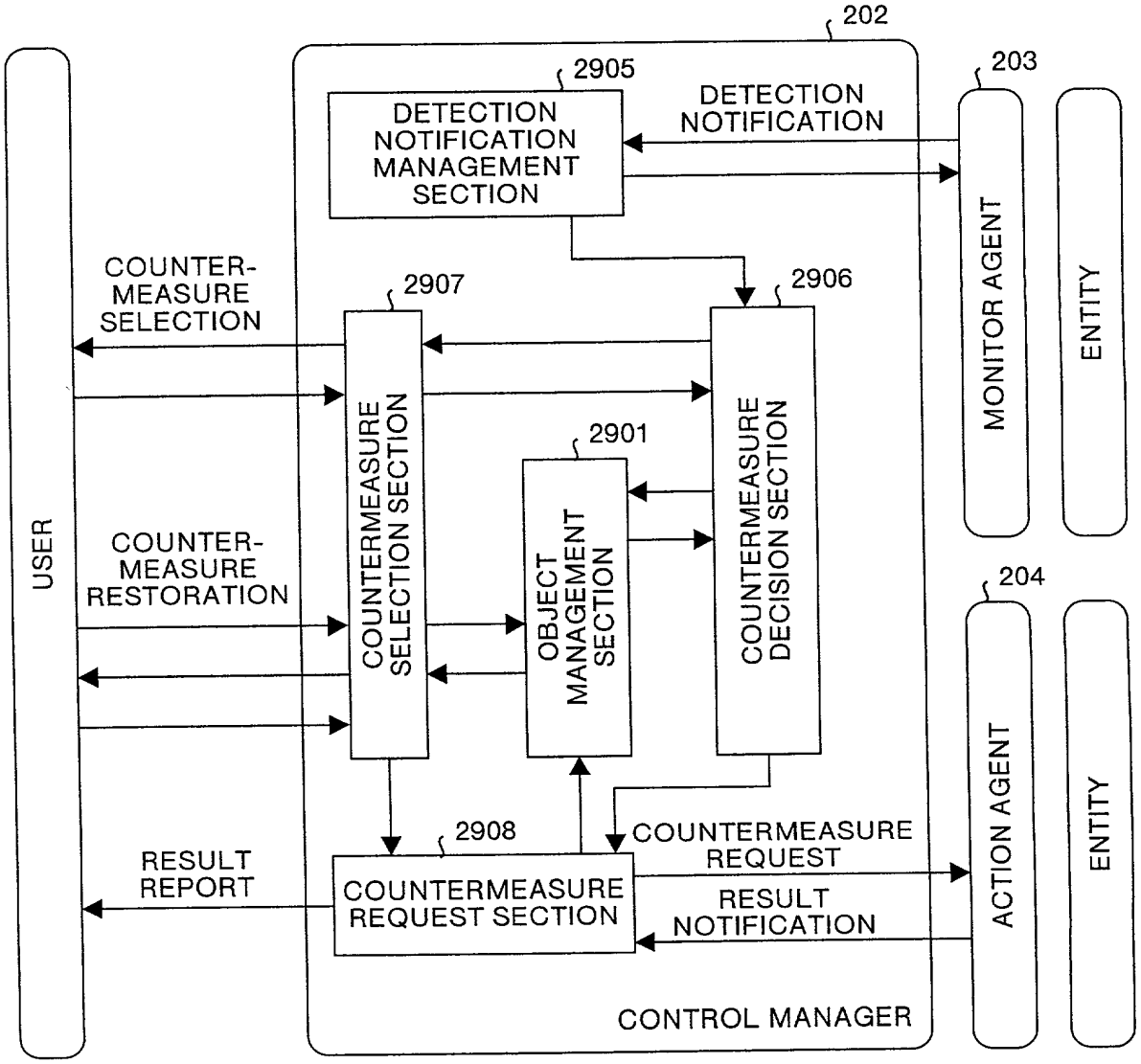

202
2905
DETECTION NOTIFICATION MANAGEMENT SECTION
DETECTION NOTIFICATION
203
MONITOR AGENT
ENTITY
USER
COUNTER-MEASURE SELECTION
2907
COUNTERMEASURE SELECTION SECTION
2906
COUNTERMEASURE DECISION SECTION
2901
OBJECT MANAGEMENT SECTION
COUNTER-MEASURE RESTORATION
204
ACTION AGENT
ENTITY
2908
COUNTERMEASURE REQUEST
RESULT REPORT
COUNTERMEASURE REQUEST SECTION
RESULT NOTIFICATION
CONTROL MANAGER

FIG.31

ATTRIBUTE		EXPLANATION
CONTROL MANAGER	ID	THE CONTROL MANAGER ASSIGNS AT THE TIME OF OBJECT DEFINITION
	IP ADDRESS	INFORMATION TO BECOME NECESSARY IN COMMUNICATION FROM AN AGENT TO THE CONTROL MANAGER. TWO PORT NUMBERS EXIST FOR THE MONITOR AGENT AND THE ACTION AGENT
	PORT NUMBER (1)	
	PORT NUMBER (2)	
	COMMUNICATION TIMEOUT VALUE	
	THE NUMBER OF COMMUNICATION RETRIES	
COUNTER-MEASURE RULE	FILE NAME (PLURAL NAMES ALLOWED)	SPECIFY THE PATH TO THE COUNTERMEASURE RULE FILE
COUNTER-MEASURE PLAN	FILE NAME	SPECIFY THE PATH TO THE COUNTERMEASURE PLAN FILE
LOG FORMAT DEFINITION	FILE NAME	THE CONTROL MANAGER DRAWS OUT TIME FROM THE ENTITY LOG SENT FROM THE MONITOR AGENT
AGENT AUTHORIZA-TION LIST	FILE NAME	THE LIST OF AN AGENT AUTHORIZED BY AN AUTHORIZATION ORGANIZATION. THE CONTROL MANAGER DOES NOT ACCEPT PROCESS FROM AN AGENT WHICH IS NOT IN THE LIST
STATE MONITOR	TIME INTERVAL	THE INTERVAL FOR CONFIRMING THE STATE OF AN AGENT IS SPECIFIED
MONITOR AGENT	ID (PLURAL IDS ALLOWED)	WHEN THE MONITOR AGENT IS OBJECT-DEFINED, IT IS AUTOMATICALLY ADDED
ACTION AGENT	ID (PLURAL IDS ALLOWED)	WHEN THE ACTION AGENT IS OBJECT-DEFINED, IT IS AUTOMATICALLY ADDED

EP 0 965 922 A2

FIG.32

ATTRIBUTE		EXPLANATION
AGENT	ID	THE CONTROL MANAGE ASSIGNS AT THE TIME OF OBJECT DEFINITION
	STATUS	SHOW THE OPERATION STATE
	IP ADDRESS	INFORMATION TO BECOME NECESSARY IN COMMUNICATION FROM THE CONTROL MANAGER TO AN AGENT
	PORT NUMBER	
	COMMUNICATION TIMEOUT VALUE	
	THE NUMBER OF COMMUNICATION RETRIES	
ENTITY	ID	OBJECT ENTITY OF AN AGENT
CONTROL MANAGER	ID	CONTROL MANAGER OF AN AGENT

FIG.33

ATTRIBUTE		EXPLANATION
ENTITY	ID	THE CONTROL MANAGE ASSIGNS AT THE TIME OF OBJECT DEFINITION
	IP ADDRESS	INFORMATION TO BECOME NECESSARY IN COMMUNICATION FROM AN AGENT TO AN ENTITY
	PORT NUMBER	
	COMMUNICATION TIME OUT VALUE	
	THE NUMBER OF COMMUNICATION RETRIES	
FW ENTITY	ID	ENTITY CORRESPONDING TO THE FIREWALL OF THE ENTITY
MONITOR AGENT	ID	WHEN THE MONITOR AGENT IS OBJECT-DEFINED, IT IS AUTOMATICALLY ADDED
ACTION AGENT	ID	WHEN THE ACTION AGENT IS OBJECT-DEFINED, IT IS AUTOMATICALLY ADDED
COUNTER-MEASURE HISTORY	(PLURALITY IS ALLOWED)	LEAVE A COUNTERMEASURE OR A COUNTERMEASURE RESULT AS A HISTORY
ENTITY INHERENT INFORMATION	FIREWALL-1	FIREWALL-1 OBJECT NAME

JP2002-259218

FIG.34

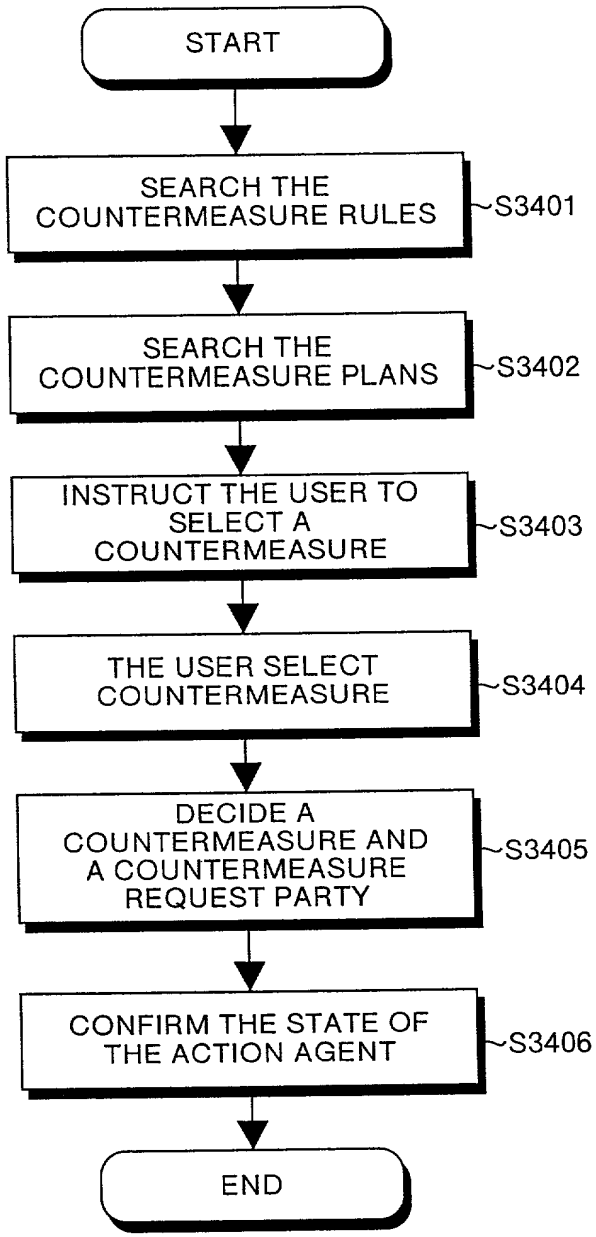

START
SEARCH THE COUNTERMEASURE RULES
S3401
SEARCH THE COUNTERMEASURE PLANS
S3402
INSTRUCT THE USER TO SELECT A COUNTERMEASURE
S3403
THE USER SELECT COUNTERMEASURE
S3404
DECIDE A COUNTERMEASURE AND A COUNTERMEASURE REQUEST PARTY
S3405
CONFIRM THE STATE OF THE ACTION AGENT
S3406
END

FIG.35

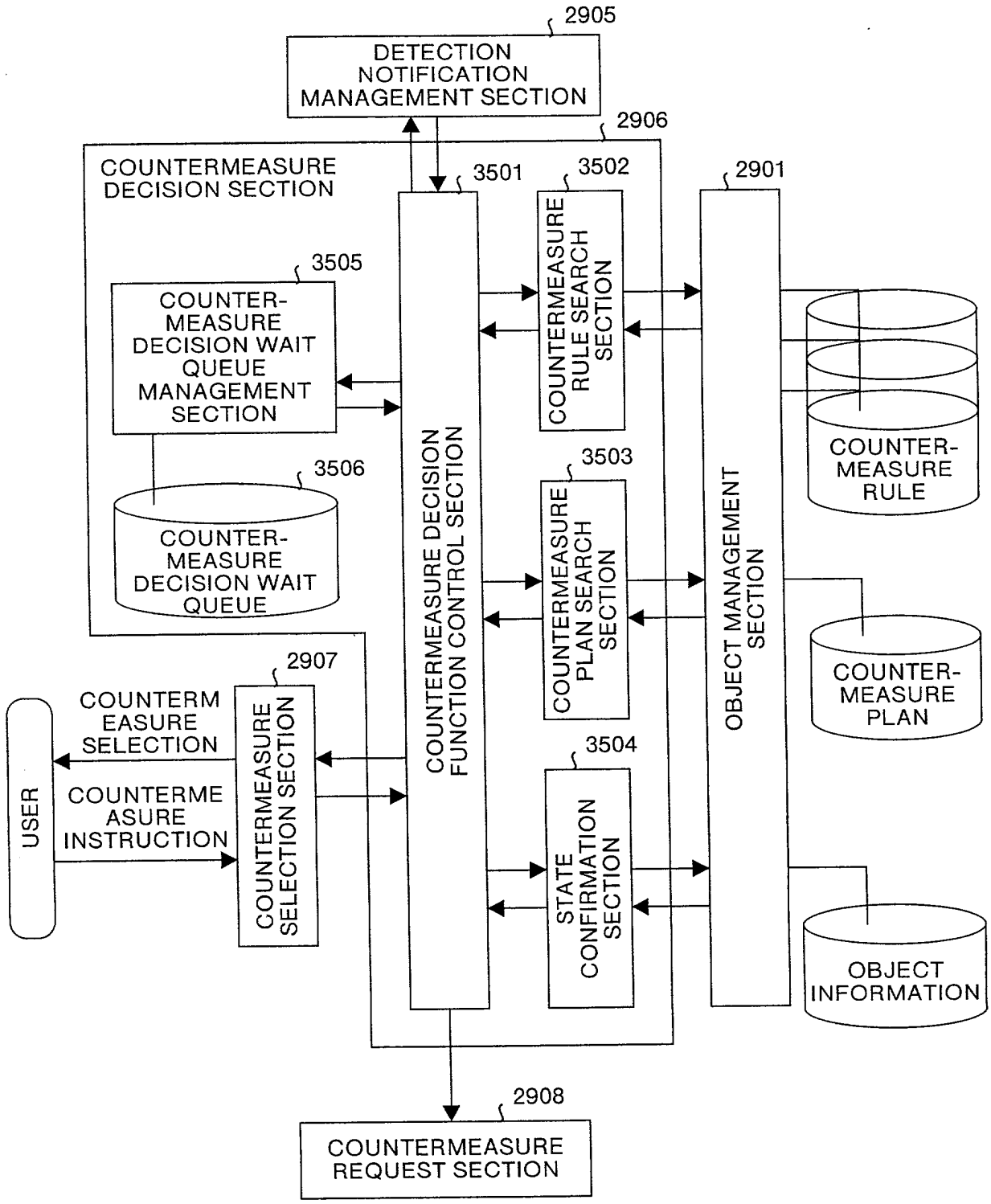

2905
DETECTION NOTIFICATION MANAGEMENT SECTION
2906
COUNTERMEASURE DECISION SECTION
3501
3502
2901
3505
COUNTER-MEASURE DECISION WAIT QUEUE MANAGEMENT SECTION
COUNTERMEASURE RULE SEARCH SECTION
COUNTER-MEASURE RULE
3506
COUNTER-MEASURE DECISION WAIT QUEUE
COUNTERMEASURE DECISION FUNCTION CONTROL SECTION
3503
COUNTERMEASURE PLAN SEARCH SECTION
OBJECT MANAGEMENT SECTION
COUNTER-MEASURE PLAN
2907
COUNTERM EASURE SELECTION
COUNTERME ASURE INSTRUCTION
USER
COUNTERMEASURE SELECTION SECTION
3504
STATE CONFIRMATION SECTION
OBJECT INFORMATION
2908
COUNTERMEASURE REQUEST SECTION

FIG.36

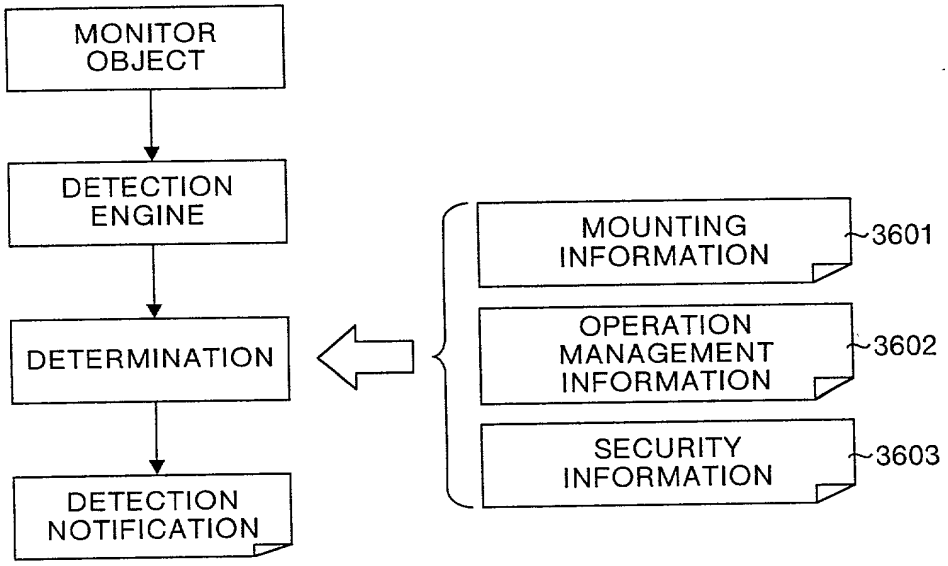
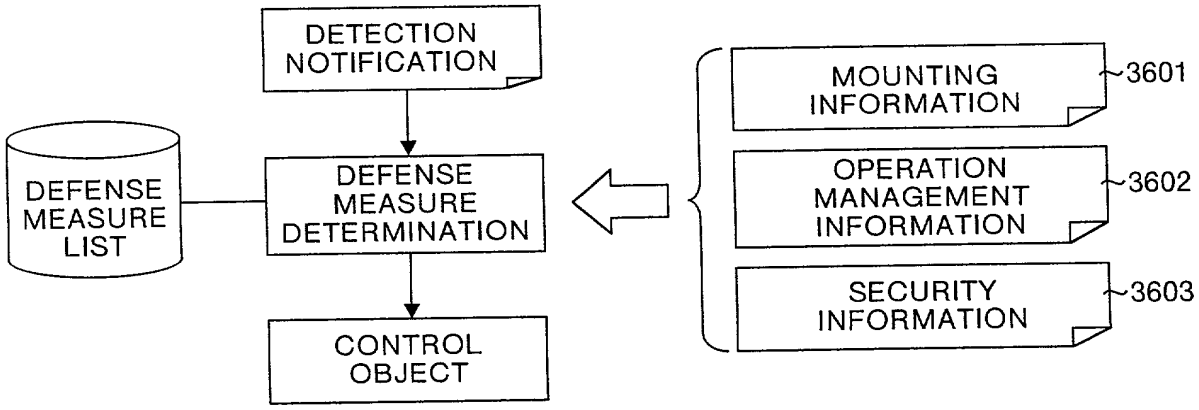


FIG.37



JP2006-259922A

FIG.38

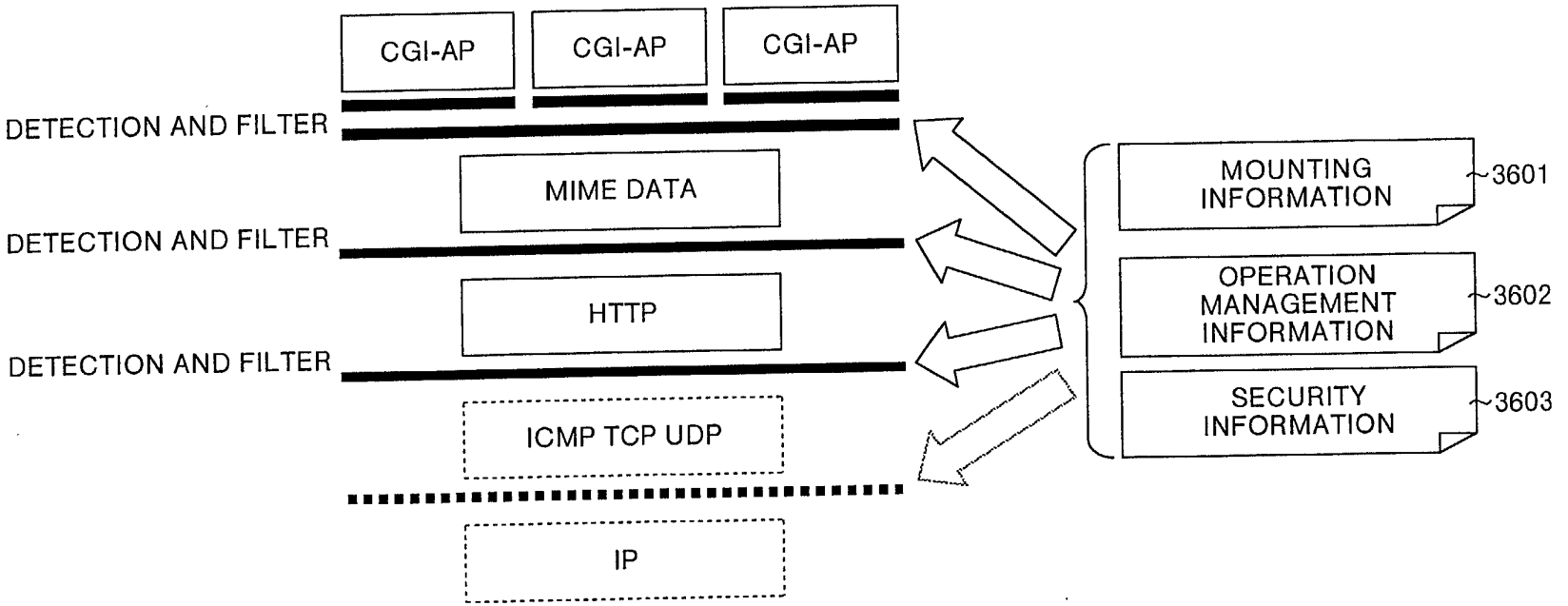
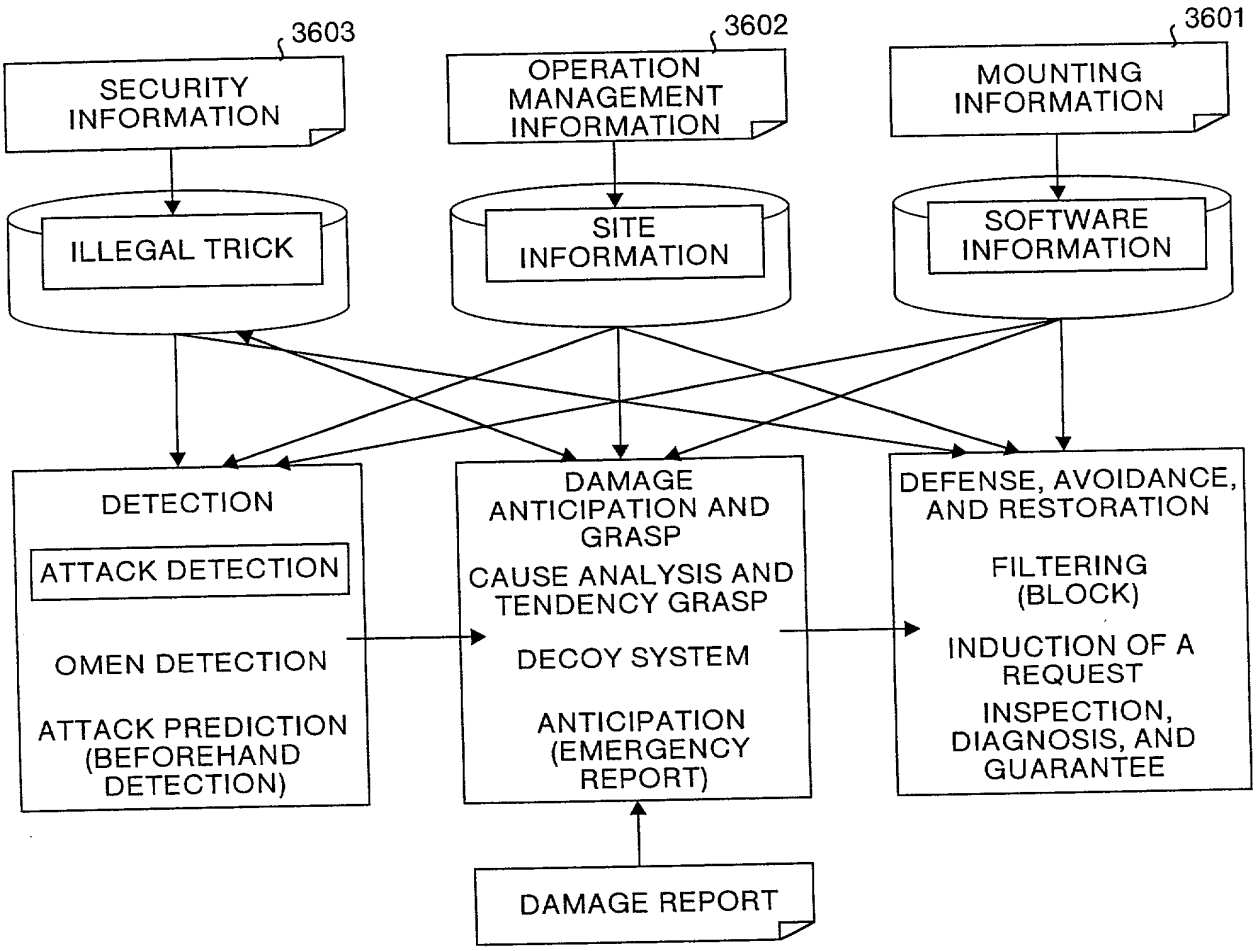

CGI-AP
CGI-AP
CGI-AP
DETECTION AND FILTER
MIME DATA
DETECTION AND FILTER
HTTP
DETECTION AND FILTER
ICMP TCP UDP
IP
MOUNTING INFORMATION
3601
OPERATION MANAGEMENT INFORMATION
3602
SECURITY INFORMATION
3603

FIG.39



EP 2 056 565 A1